

Manipulation of Ideals

The goal of this lecture is to show how Gröbner basis provide algorithms for basic ideal manipulations. Our main reference is [2, Chapter 4]. In [1] we find more explicit descriptions of the algorithms. The application comes from algebraic statistics.

1 Radicals Ideals

We consider an ideal I generated by N polynomials $f_i \in \mathbb{K}[x_1, x_2, \dots, x_n] = \mathbb{K}[\mathbf{x}]$, \mathbb{K} is an algebraically closed field, $i = 1, 2, \dots, N$:

$$I = \langle f_1, f_2, \dots, f_N \rangle = \{ a_1 f_1 + a_2 f_2 + \dots + a_N f_N \mid a_i \in \mathbb{K}[\mathbf{x}] \}. \quad (1)$$

The variables involved in the polynomial ring matter. An ideal I in $\mathbb{K}[\mathbf{x}]$ is not an ideal in $\mathbb{K}[\mathbf{x}, \mathbf{y}]$ because it is not closed under multiplication with variables in \mathbf{y} . Introducing a new variable is a useful technique, for example to solve the radical ideal membership problem.

For any ideal I , its radical is

$$\sqrt{I} = \{ p \in \mathbb{K}[\mathbf{x}] \mid p^k \in I \text{ for some } k \in \mathbb{N} \}. \quad (2)$$

One motivation to introduce Gröbner bases was to solve the ideal membership problem. The problem to determine whether a polynomial belongs to the radical of an ideal is by Theorem 1.1 reduced to the regular ideal membership problem, solved by the division (or normal form) algorithm when the ideal is generated by a Gröbner basis.

Theorem 1.1 (radical ideal membership) *Let $I = \langle f_1, f_2, \dots, f_N \rangle$ be an ideal in $\mathbb{K}[\mathbf{x}]$ and $f \in \mathbb{K}[\mathbf{x}]$.*

$$f \in \sqrt{I} \Leftrightarrow 1 \in J := \langle f_1, f_2, \dots, f_N, 1 - yf \rangle. \quad (3)$$

Proof. To show the \Rightarrow direction, we have $f \in \sqrt{I}$: there is a power $k \geq 1$: $f^k \in I$. As $I \subset J$: $f^k \in J$. We use k to show that $1 \in J$:

$$1 = 1 - y^k f^k + y^k f^k \quad (4)$$

$$= \underbrace{(1 - yf)(1 + yf + \dots + y^{k-1} f^{k-1})}_{\in J} + y^k \underbrace{f^k}_{\in J} \quad (5)$$

$$\in J. \quad (6)$$

For the \Leftarrow direction, we have $1 \in J$:

$$1 = \sum_{i=1}^N p_i(\mathbf{x}, y) f_i(\mathbf{x}) + b(\mathbf{x}, y)(1 - yf(\mathbf{x})), y = 1/f \quad (7)$$

$$= \sum_{i=1}^N p_i(\mathbf{x}, 1/f) f_i(\mathbf{x}). \quad (8)$$

To clear all denominators of $p_i(\mathbf{x}, 1/f)$, use a power k of f . Denoting the polynomials with cleared denominators as $P_i(\mathbf{x})$:

$$f^k = \sum_{i=1}^N P_i(\mathbf{x}) f_i(\mathbf{x}). \quad (9)$$

Thus $f \in \sqrt{I}$. □

To verify that an ideal is radical, we use the following

Proposition 1.1 *Let I be an ideal and $<$ be any term order. If the initial monomial ideal $\text{in}_{<}(I)$ is square free, then I is a radical ideal.*

One definition of a Gröbner basis G is that $\text{in}_{<}(G)$ generates the initial ideal $\text{in}_{<}(I)$ so if all polynomials $g \in G$ are square free, then I is radical. So a Gröbner basis provides an effective version of the proposition.

2 Independence Varieties

Following [3, Chapter 8], we consider a conditional independence statement denoted as

$$A \perp B \mid C \quad \text{meaning: } A \text{ is independent of } B \text{ given } C. \quad (10)$$

An independence statement translates into a set of quadratic polynomials. We illustrate this with $A \perp B \mid C$. Suppose that A , B , and C are discrete random variables with each take two outcomes in $\{0, 1\}$. The statement

$$\text{for all } i, j, k \in \{0, 1\} : \text{Prob}(A = i, B = j \mid C = k) = \text{Prob}(A = i \mid C = k) \times \text{Prob}(B = j \mid C = k) \quad (11)$$

says that the probability of $A = i$ and $B = j$, given $C = k$, is the product of the probabilities that A and B separately equal i and j respectively, given $C = k$. This probability statement expresses $A \perp B \mid C$.

Denoting $p_{ijk} = \text{Prob}(A = i, B = j, C = k)$, for $i, j, k \in \{0, 1\}$ introduces eight indeterminates. Via $\text{Prob}(A = i \mid C = k) = \text{Prob}(A = i, C = k) / \text{Prob}(C = k)$ we remove the conditional probabilities. The statement A is independent of B given C gives rise to the prime ideal

$$I_{A \perp B \mid C} = \langle p_{000}p_{011} - p_{001}p_{010}, p_{100}p_{111} - p_{101}p_{110} \rangle. \quad (12)$$

Its variety $V(I_{A \perp B \mid C})$ is an independence variety. The generators of $I_{A \perp B \mid C}$ are 2-by-2 minors of

$$\begin{bmatrix} p_{000} & p_{010} & p_{100} & p_{110} \\ p_{001} & p_{011} & p_{101} & p_{111} \end{bmatrix}. \quad (13)$$

3 Zariski Closure

Usually, we assume as given an ideal $I = \langle f_1, f_2, \dots, f_N \rangle$ of $\mathbb{K}[\mathbf{x}]$ and then consider $V = V(I)$ as the solution set of the system $f(\mathbf{x}) = \mathbf{0}$, defined by the polynomials f_i , $i = 1, 2, \dots, N$. In reverse, we consider as given a set $S \subset \mathbb{K}^n$ and consider

$$I(S) = \{ f \in \mathbb{K}[\mathbf{x}] \mid f(\mathbf{z}) = 0 \text{ for all } \mathbf{z} \in S \}. \quad (14)$$

For a set S , we define $\overline{S} = V(I(S))$ as the Zariski closure of S . \overline{S} is the smallest variety that contains S .

Proposition 3.1 *For $S \subset \mathbb{K}^n$, $V(I(S))$ is the smallest variety that contains S .*

Note that for $W \supset S$: $I(W) \subset I(S)$ and $I(S)$ is a radical ideal.

Elimination ideals are natural examples to illustrate Zariski closure. A Gröbner basis with a lexicographical term order provides a basis for an elimination ideal.

Theorem 3.1 *Let $I = \langle f_1, f_2, \dots, f_N \rangle$ be an ideal in $\mathbb{K}[\mathbf{x}]$ with solution set $V = V(I)$. Let $\pi_\ell : \mathbb{K}^n \rightarrow \mathbb{K}^{n-\ell}$ be the projection onto the last $n - \ell$ components. Let $I_\ell = I \cap \mathbb{K}[x_{\ell+1}, \dots, x_n]$ be the ℓ th elimination ideal. Then $V(I_\ell)$ is the Zariski closure of $\pi_\ell(V)$.*

4 Intersection of Ideals

Given two ideals I and J in $\mathbb{K}[\mathbf{x}]$, we define their sum, product and intersection respectively as

$$I + J = \{ f + g \mid f \in I \text{ and } g \in J \} \quad (15)$$

$$I \cdot J = \{ f \cdot g \mid f \in I \text{ and } g \in J \} \quad (16)$$

$$I \cap J = \{ f \in \mathbb{K}[\mathbf{x}] \mid f \in I \text{ and } f \in J \}. \quad (17)$$

We leave it as an exercise to show that $I + J$, $I \cdot J$, and $I \cap J$ are ideals in $\mathbb{K}[\mathbf{x}]$.

Good examples are monomial ideals. For example, consider $I = \langle x^2y \rangle$. It is not too hard to see – think about the staircase representation of monomial ideals – that $I = \langle x^2 \rangle \cap \langle y \rangle$. For $J = \langle xy^2 \rangle$, $I \cdot J = \langle x^2y, xy^2 \rangle$ and $I \cap J = \langle x^2y^2 \rangle$. For general exponents $\mathbf{a}, \mathbf{b} \in \mathbb{N}^n$: $\langle \mathbf{x}^{\mathbf{a}} \rangle \cap \langle \mathbf{x}^{\mathbf{b}} \rangle = \langle \mathbf{x}^{\mathbf{c}} \rangle$, where \mathbf{c} is the least common multiple of \mathbf{a} and \mathbf{b} .

Given generators for I and J , we consider the problem of computing generators for $I \cap J$.

Theorem 4.1 For I and J ideals in $\mathbb{K}[\mathbf{x}]$:

$$I \cap J = (tI + (1-t)J) \cap \mathbb{K}[\mathbf{x}]. \quad (18)$$

Proof. We show the equality = via containments \subseteq and \supseteq .

\subseteq $f \in I \cap J$ implies $f \in I$ and $f \in J$ and thus also $tf \in tI$ and $(1-t)f \in (1-t)J$. Thus we can write f as $f = tf + (1-t)f \in tf + (1-t)J$. Since I and J are ideals in $\mathbb{K}[\mathbf{x}]$, we have $f \in (tI + (1-t)J) \cap \mathbb{K}[\mathbf{x}]$.

\supseteq $f \in (tI + (1-t)J) \cap \mathbb{K}[\mathbf{x}]$ implies $f(\mathbf{x}) = g(\mathbf{x}, t) + h(\mathbf{x}, t)$, for $g \in tI$ and $h \in (1-t)J$. We show that $f \in J$ by setting $t = 0$. Because every element in tI is a multiple of t : $g(\mathbf{x}, 0) = 0$ and therefore: $f(\mathbf{x}) = h(\mathbf{x}, 0)$. Now we have to show that $h(\mathbf{x}, 0) \in J$. Let $J = \langle j_1, j_2, \dots, j_N \rangle$, then for any $h \in (1-t)J$: $h(\mathbf{x}, t) = (1-t)(a_1(\mathbf{x})j_1(\mathbf{x}) + a_2(\mathbf{x})j_2(\mathbf{x}) + \dots + a_N(\mathbf{x})j_N(\mathbf{x}))$, for $a_i \in \mathbb{K}[\mathbf{x}]$. As $h(\mathbf{x}, 0) = a_1(\mathbf{x})j_1(\mathbf{x}) + a_2(\mathbf{x})j_2(\mathbf{x}) + \dots + a_N(\mathbf{x})j_N(\mathbf{x}) \in J$, we have $f \in J$. Similarly, we can show that $f \in I$ by setting $t = 1$. Thus $f \in I \cap J$. \square

The importance of the theorem is that it leads to an algorithm to compute the generators of $I \cap J$. Let $I = \langle i_1, i_2, \dots, i_r \rangle$ and $J = \langle j_1, j_2, \dots, j_s \rangle$ be ideals in $\mathbb{K}[\mathbf{x}]$. Then consider

$$K = \langle ti_1, ti_2, \dots, ti_r, (1-t)j_1, (1-t)j_2, \dots, (1-t)j_s \rangle \subset \mathbb{K}[\mathbf{x}, t]. \quad (19)$$

A Gröbner basis of K with respect to any lexicographical order for which t is greater than any variable in \mathbf{x} will give a Gröbner basis for $I \cap J$.

In Macaulay 2, the command to intersect ideals is `intersect`. From the documentation, we copy the input statements:

```
i1 : R = QQ[a..d];
i2 : intersect(ideal(a,b),ideal(c*d,a*b),ideal(b*d,a*c))

o3 = ideal (b*c*d, a*c*d, a*b*d, a*b*c)
```

When we pass to the solution set, the intersection turns into a union.

Theorem 4.2 For I and J ideals in $\mathbb{K}[\mathbf{x}]$: $V(I \cap J) = V(I) \cup V(J)$.

Proof. We proceed proving the = in two steps: first \subseteq and then \supseteq .

$$\mathbf{z} \in V(I) \cup V(J) \Rightarrow \mathbf{z} \in V(I) \text{ or } \mathbf{z} \in V(J) \quad (20)$$

$$\Rightarrow f(\mathbf{z}), f \in I \text{ or } f(\mathbf{z}), f \in J \quad (21)$$

So for $f \in I \cap J$: $f(\mathbf{z}) = \mathbf{0}$, thus $V(I) \cup V(J) \subseteq V(I \cap J)$.

For \supseteq , observe $V(I \cdot J) = V(I) \cup V(J)$. We first show $I \cdot J \subset I \cap J$. For $f \in I \cdot J$: $f = gh$, $g \in I$ and $h \in J$. Because I is an ideal, $g \in I$ and $h \in \mathbb{K}[\mathbf{x}]$ implies $gh = f \in I$. Likewise, because J is an ideal, $f \in J$, so we have $f \in I \cap J$. Then $I \cdot J \subset I \cap J$ implies $V(I \cdot J) \supset V(I \cap J)$ and we have \supseteq . \square

5 Quotient of Ideals

Let I and J be ideals in $\mathbb{K}[\mathbf{x}]$, the ideal quotient of I and J (or colon ideal) is

$$I : J = \{ f \in \mathbb{K}[\mathbf{x}] : fg \in I \text{ for all } g \in J \}. \quad (22)$$

We leave it as an exercise that $I : J$ is an ideal in $\mathbb{K}[\mathbf{x}]$ and that $I \subset I : J$.

An example with monomial ideals justifies the name quotient:

$$\langle xz, yz \rangle : \langle z \rangle = \{ f \in \mathbb{K}[x, y, z] : f \cdot z \in \langle xz, yz \rangle \}, \quad (23)$$

$$= \{ f \in \mathbb{K}[x, y, z] : f \cdot z = a_1xz + a_2yz, a_1, a_2 \in \mathbb{K}[x, y, z] \}, \quad (24)$$

$$= \{ f \in \mathbb{K}[x, y, z] : f = a_1x + a_2y, a_1, a_2 \in \mathbb{K}[x, y, z] \}, \quad (25)$$

$$= \langle x, y \rangle. \quad (26)$$

The quotient $I : J$ can be computed via the intersection of quotient of I with the generators of J , formally denoted as

$$I : \langle f_1, f_2, \dots, f_N \rangle = \bigcap_{i=1}^N (I : f_i). \quad (27)$$

To justify this formula, we need to show that $I : (J + K) = I : J \cap I : K$ for ideals I , J , and K .

To compute $I : \langle f \rangle$, we use the following theorem:

Theorem 5.1 *Let I be an ideal in $\mathbb{K}[\mathbf{x}]$ and $f \in \mathbb{K}[\mathbf{x}]$. If $\{g_1, g_2, \dots, g_s\}$ is a basis of $I \cap \langle f \rangle$, then $\{g_1/f, g_2/f, \dots, g_s/f\}$ is a basis of $I : \langle f \rangle$.*

Proof. We first show that any element in $\left\langle \frac{g_1}{f}, \frac{g_2}{f}, \dots, \frac{g_s}{f} \right\rangle$ belongs to $I : \langle f \rangle$. We have:

$$q \in \left\langle \frac{g_1}{f}, \frac{g_2}{f}, \dots, \frac{g_s}{f} \right\rangle \Rightarrow fq \in \langle g_1, g_2, \dots, g_s \rangle = I \cap \langle f \rangle. \quad (28)$$

Applying the definition of $I : \langle f \rangle = \{ a \in \mathbb{K}[\mathbf{x}] : ap \in I, \text{ for all } p \in \langle f \rangle \}$. For q to belong in $I : \langle f \rangle$, we must have that $qp \in I$ for all $p \in \langle f \rangle$. As $p \in \langle f \rangle$, $p = bf$, for some $b \in \mathbb{K}[\mathbf{x}]$. So $qp = qbf$ and $q \in I \cap \langle f \rangle \subset I$. Thus $q \in I : \langle f \rangle$.

We still have to show that every $q \in I : \langle f \rangle$ is a polynomial combination of $\left\{ \frac{g_1}{f}, \frac{g_2}{f}, \dots, \frac{g_s}{f} \right\}$. For $q \in I : \langle f \rangle$, we have: $fq \in I$. Since $fq \in \langle f \rangle$, we have $fq \in I \cap \langle f \rangle$, so $fq = a_1g_1 + a_2g_2 + \dots + a_sg_s$, for $a_i \in \mathbb{K}[\mathbf{x}]$, $i = 1, 2, \dots, s$, as $\langle g_1, g_2, \dots, g_s \rangle = I \cap \langle f \rangle$. Because each $g_i \in \langle f \rangle$, each g_i/f is a polynomial, and we have $q = a_1 \frac{g_1}{f} + a_2 \frac{g_2}{f} + \dots + a_s \frac{g_s}{f}$. \square

The theorem gives an algorithm to compute $I : J$ for $J = \langle j_1, j_2, \dots, j_s \rangle$, using (27).

In Macaulay 2, copying from the online documentation, we compute the quotient of two ideals via the colon operator (the command `quotient` allows the user to give options):

```

i1 : R = QQ[a..d];
i2 : I = ideal(a^2*b-c^2,a*b^2-d^3,c^5-d);
i3 : J = ideal(a^2,b^2,c^2,d^2);
i4 : I:J
      2   3   2   2   5
o4 = ideal (a*b  - d , a b - c , c  - d)

```

6 Saturation

The saturation of I by p is

$$(I : p^\infty) = \{ q \in \mathbb{K}[\mathbf{x}] \mid qp^N \in I, \text{ for some } N \}. \quad (29)$$

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

Via Gröbner bases we may compute $(I : p^\infty)$ as follows. Let

$$J = I + (tp - 1) \in \mathbb{K}[t, \mathbf{x}], \quad \text{then} \quad (I : p^\infty) = J \cap \mathbb{K}[\mathbf{x}]. \quad (30)$$

Gröbner bases with a lexicographical term order eliminate. The Macaulay 2 command for saturation is `saturate`.

7 An Algebra-Geometry Dictionary

Table 1 is an adaption of [2, §8], summarizing the background for this lecture.

algebra	\leftrightarrow	geometry
radical ideal $I = \sqrt{I}$	\rightarrow	$V(I)$ variety
$I(V)$ ideal of a set	\leftarrow	solution set V
sum of ideals $I + J$	\rightarrow	$V(I) \cap V(J)$ intersection of varieties
$\sqrt{I(V) + I(W)}$ radical of sum	\leftarrow	intersection of sets $V \cap W$
product of ideals IJ	\rightarrow	$V(I) \cup V(J)$ union of varieties
$\sqrt{I(V)I(W)}$ radical of product	\leftarrow	union of sets $V \cup W$
intersection of ideals $I \cap J$	\rightarrow	$V(I) \cup V(J)$ union of varieties
$I(V) \cap I(W)$	\leftarrow	union of sets $V \cup W$
quotient of ideals $I : J$	\rightarrow	$\overline{V(I) - V(J)}$ difference of varieties
$I(V) : I(W)$	\leftarrow	difference of sets $\overline{V - W}$
elimination $\sqrt{I \cap \mathbb{C}[x_{k+1}, \dots, x_n]}$	\leftrightarrow	$\overline{\pi_k(V(I))}$ projection of varieties

Table 1: The Algebra-Geometry Dictionary.

8 Exercises

1. For ideals I and J in $\mathbb{K}[\mathbf{x}]$, show that $I + J$, $I \cdot J$ and $I \cap J$ are ideals in $\mathbb{K}[\mathbf{x}]$.
2. For $I = J = \langle x, y \rangle$, show that $I \cdot J \subsetneq I \cap J$.

3. Let $I = \langle x_1x_4 + x_2x_3, x_1x_3, x_2x_4 \rangle$. Compute $(I : x_4^2)$.
4. Show that $V(I \cap J) = V(I) \cup V(J)$ for ideals I and J in $\mathbb{K}[\mathbf{x}]$.

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] D. Cox, J. Little, and D. O’Shea. *Ideals, Varieties and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Undergraduate Texts in Mathematics. Springer-Verlag, second edition, 1997.
- [3] B. Sturmfels. *Solving Systems of Polynomial Equations*. Number 97 in CBMS Regional Conference Series in Mathematics. AMS, 2002.