

Computational Algebra

Songyu Ye

December 4, 2024

Abstract

We prepare notes about Groebner basis and their applications. We will use Macaulay2 to solve problems related to ideals, varieties, and Groebner bases. These notes are based on the book ‘Ideals, Varieties, and Algorithms’ by Cox, Little, and O’Shea, and were prepared for the final exam of Math 4370 at Cornell University, taught by Professor Rachel Webb.

Contents

1	Groebner bases	2
1.1	Ideal membership	2
2	Elimination theory	3
3	Families of varieties	5
3.1	Implicit and parametric representations	5
3.2	Envelopes	7
4	Radical ideals	8
4.1	Big theorems	9
4.2	Radical ideal problem	10
4.3	Radical membership problem	10
5	Product and intersection of ideals	11
6	Graph algorithms and integer programming	13
6.1	Chromatic number	13
6.2	Minimal vertex cover	14
6.3	Integer programming	16
7	Groebner degeneration and flatness	20
8	Affine vs. projective flatness	22

1 Gröbner bases

Let k be an algebraically closed field. We have the following result about Gröbner bases, essentially because of their property of unique division.

Proposition 1.1. *Fix a monomial ordering on $k[x_1, \dots, x_n]$ and let $I \subseteq k[x_1, \dots, x_n]$ be an ideal.*

1. *Every $f \in k[x_1, \dots, x_n]$ is congruent modulo I to a unique polynomial r which is a k -linear combination of the monomials in the complement of $\langle \text{LT}(I) \rangle$.*
2. *The elements of $\{x^\alpha \mid x^\alpha \notin \langle \text{LT}(I) \rangle\}$ are “linearly independent modulo I ,” i.e., if we have*

$$\sum_{\alpha} c_{\alpha} x^{\alpha} \equiv 0 \pmod{I},$$

where the x^{α} are all in the complement of $\langle \text{LT}(I) \rangle$, then $c_{\alpha} = 0$ for all α .

In particular this implies that we can calculate $\dim R/I$ by counting the number of monomials not in $\langle \text{LT}(I) \rangle$.

Theorem 1.2 (Finiteness Theorem). *Let $I \subseteq k[x_1, \dots, x_n]$ be an ideal and fix a monomial ordering on $k[x_1, \dots, x_n]$. The following are equivalent:*

- (i) *For each i , $1 \leq i \leq n$, there is some $m_i \geq 0$ such that $x_i^{m_i} \in \langle \text{LT}(I) \rangle$.*
- (ii) *Let G be a Gröbner basis for I . Then for each i , $1 \leq i \leq n$, there is some $m_i \geq 0$ such that $x_i^{m_i} = \text{LM}(g)$ for some $g \in G$.*
- (iii) *The set $\{x^\alpha \mid x^\alpha \notin \langle \text{LT}(I) \rangle\}$ is finite.*
- (iv) *The k -vector space $k[x_1, \dots, x_n]/I$ is finite-dimensional.*
- (v) *$V(I) \subseteq k^n$ is a finite set.*

1.1 Ideal membership

The existence of a Gröbner basis also allows us to determine whether a polynomial is in an ideal.

Algorithm for ideal membership 1:

Input: An ideal $I \subseteq k[x_1, \dots, x_n]$, a polynomial $f \in k[x_1, \dots, x_n]$.

Output: Determine whether $f \in I$.

Steps:

1. Compute a Gröbner basis G for I .
2. Use the division algorithm to divide f by G .
3. If the remainder is zero, then $f \in I$. Otherwise, $f \notin I$.

Problem 1: Is $x^{11} - x$ in the ideal $I = \langle xy^3 - x^2, x^3y^2 - y \rangle$?

Solution. We compute a Gröbner basis for the ideal given using the grevlex order:

```
R = QQ[x, y, z]
G = gens gb ideal (x*y^3 - x^2, x^3*y^2 - y)
```

The Gröbner basis found by the computation is:

$$G = \{y^4 - x^2y, xy^3 - x^2, x^4 - y^2, x^3y^2 - y\}.$$

Then we use the division algorithm to divide $x^{11} - x$ by the Gröbner basis:

```
divisionAlgo (x^11 - x, flatten entries G)
```

The output of this computation shows that the remainder is $y^3 - x$, which is not zero. Since the remainder is nonzero, this demonstrates that $x^{11} - x$ is **not** in the ideal I .

Answer: No.

2 Elimination theory

Recall these theorems from the book:

Theorem 2.1 (The Elimination Theorem). *Let $I \subseteq k[x_1, \dots, x_n]$ be an ideal and let G be a Gröbner basis of I with respect to lexicographic order where $x_1 > x_2 > \dots > x_n$. Then, for every $0 \leq l \leq n$, the set*

$$G_l = G \cap k[x_{l+1}, \dots, x_n]$$

is a Gröbner basis of the l -th elimination ideal I_l .

Proof. Fix l between 0 and n . Since $G_l \subseteq I_l$ by construction, it suffices to show that

$$\langle \text{LT}(I_l) \rangle = \langle \text{LT}(G_l) \rangle$$

by the definition of Gröbner basis. One inclusion is obvious, and to prove the other inclusion $\langle \text{LT}(I_l) \rangle \subseteq \langle \text{LT}(G_l) \rangle$, we need only to show that the leading term $\text{LT}(f)$, for an arbitrary $f \in I_l$, is divisible by $\text{LT}(g)$ for some $g \in G_l$. To prove this, note that f also lies in I , which tells us that $\text{LT}(f)$ is divisible by $\text{LT}(g)$ for some $g \in G$ since G is a Gröbner basis of I . Since $f \in I_l$, this means that $\text{LT}(g)$ involves only the variables x_{l+1}, \dots, x_n . Now comes the crucial observation: since we are using lexicographic order with $x_1 > \dots > x_n$, any monomial involving x_1, \dots, x_l is greater than all monomials in $k[x_{l+1}, \dots, x_n]$, so that $\text{LT}(g) \in k[x_{l+1}, \dots, x_n]$ implies $g \in G_l$. This shows that $g \in G_l$, and the theorem is proved. \square

Theorem 2.2 (The Extension Theorem). Let $I = \langle f_1, \dots, f_s \rangle \subseteq \mathbb{C}[x_1, \dots, x_n]$ and let I_1 be the first elimination ideal of I . For each $1 \leq i \leq s$, write f_i in the form

$$f_i = c_i(x_2, \dots, x_n)x_1^{N_i} + \text{terms in which } x_1 \text{ has degree} < N_i,$$

where $N_i \geq 0$ and $c_i \in \mathbb{C}[x_2, \dots, x_n]$ is nonzero. Suppose that we have a partial solution $(a_2, \dots, a_n) \in V(I_1)$. If $(a_2, \dots, a_n) \notin V(c_1, \dots, c_s)$, then there exists $a_1 \in \mathbb{C}$ such that $(a_1, a_2, \dots, a_n) \in V(I)$.

Theorem 2.3 (The Closure Theorem). Let $V = V(f_1, \dots, f_s) \subseteq \mathbb{C}^n$ and let I_l be the l -th elimination ideal of $\langle f_1, \dots, f_s \rangle$. Then:

1. $V(I_l)$ is the smallest affine variety containing $\pi_l(V) \subseteq \mathbb{C}^{n-l}$.
2. When $V \neq \emptyset$, there is an affine variety $W \subseteq V(I_l)$ such that $V(I_l) \setminus W \subseteq \pi_l(V)$.

Problem 2: Solve the following system of polynomial equations using the theory of elimination ideals:

$$x^2 + 2y^2 = 2, \quad x^2 + xy + y^2 = 2.$$

Solution. We create a polynomial ring with the lex order:

```
R = QQ[x, y, MonomialOrder => Lex]
```

so that we can compute elimination ideals. We next compute a Gröbner basis:

```
gens gb ideal(x^2 + 2*y^2 - 2, x^2 + x*y + y^2 - 2)
```

The output is:

$$3y^3 - 2y, \quad x^2y - y^2, \quad x^2 + 2y^2 - 2.$$

It follows that the first elimination ideal (where we eliminate x) is generated by $3y^3 - 2y$. Solving the equation $3y^3 - 2y = 0$ yields solutions:

$$y = 0, \quad y = \sqrt{\frac{2}{3}}, \quad y = -\sqrt{\frac{2}{3}}.$$

- If $y = 0$, the first two polynomials in the Gröbner basis vanish, and the last tells us that $x = \sqrt{2}$ or $x = -\sqrt{2}$.
- If $y = \sqrt{\frac{2}{3}}$ or $y = -\sqrt{\frac{2}{3}}$, the second equation in the Gröbner basis tells us that $x = y$. One can check that this is also consistent with the last equation.

Therefore, the solutions are:

$$(\sqrt{2}, 0), \quad (-\sqrt{2}, 0), \quad \left(\sqrt{\frac{2}{3}}, \sqrt{\frac{2}{3}}\right), \quad \left(-\sqrt{\frac{2}{3}}, -\sqrt{\frac{2}{3}}\right).$$

3 Families of varieties

3.1 Implicit and parametric representations

Theorem 3.1 (Polynomial Implicitization). *If k is an infinite field, let $F : k^m \rightarrow k^n$ be the function determined by the polynomial parametrization:*

$$x_i = f_i(t_1, \dots, t_m), \quad 1 \leq i \leq n.$$

Let I be the ideal

$$I = \langle x_1 - f_1, \dots, x_n - f_n \rangle \subseteq k[t_1, \dots, t_m, x_1, \dots, x_n],$$

and let $I_m = I \cap k[x_1, \dots, x_n]$ be the m -th elimination ideal. Then $V(I_m)$ is the smallest variety in k^n containing $F(k^m)$.

Proof. By Equation (4) above and Lemma 1 of §2, $F(k^m) = \pi_m(V) \subseteq V(I_m)$. Thus $V(I_m)$ is a variety containing $F(k^m)$. To show it is the smallest, suppose that $h \in k[x_1, \dots, x_n]$ vanishes on $F(k^m)$. We show that $h \in I_m$ as follows. Divide h by $x_1 - f_1, \dots, x_n - f_n$ using lexicographic order with $x_1 > \dots > x_n > t_1 > \dots > t_m$. This gives an equation:

$$h(x_1, \dots, x_n) = q_1 \cdot (x_1 - f_1) + \dots + q_n \cdot (x_n - f_n) + r(t_1, \dots, t_m),$$

since $\text{LT}(x_j - f_j) = x_j$. Given any $a = (a_1, \dots, a_m) \in k^m$, we substitute $t_i = a_i$ and $x_i = f_i(a)$ into the above equation to obtain:

$$0 = h(f_1(a), \dots, f_n(a)) = 0 + \dots + 0 + r(a).$$

It follows that $r(a) = 0$ for all $a \in k^m$. Since k is infinite, Proposition 5 of Chapter 1, §1 implies that $r(t_1, \dots, t_m)$ is the zero polynomial. Thus we obtain:

$$h(x_1, \dots, x_n) = q_1 \cdot (x_1 - f_1) + \dots + q_n \cdot (x_n - f_n) \in I \cap k[x_1, \dots, x_n] = I_m.$$

Now suppose that $Z = V(h_1, \dots, h_s) \subseteq k^n$ is a variety of k^n such that $F(k^m) \subseteq Z$. Then each h_i vanishes on $F(k^m)$ and hence lies in I_m by the previous paragraph. Thus $V(I_m) \subseteq V(h_1, \dots, h_s) = Z$. This proves that $V(I_m)$ is the smallest variety of k^n containing $F(k^m)$. \square

Implicitization Algorithm for Polynomial Parametrizations 2:

Input: Polynomials $f_1, \dots, f_n \in k[t_1, \dots, t_m]$ defining a map $x_i = f_i(t_1, \dots, t_m)$ for $1 \leq i \leq n$.

Output: The smallest variety $V(I_m) \subseteq k^n$ containing the image of the parametrization.

Steps:

1. Define the ideal:

$$I = \langle x_1 - f_1, \dots, x_n - f_n \rangle \subseteq k[t_1, \dots, t_m, x_1, \dots, x_n].$$

2. Choose a lexicographic monomial order such that:

$$t_1 > t_2 > \cdots > t_m > x_1 > x_2 > \cdots > x_n.$$

3. Compute a Gröbner basis G for the ideal I with respect to the chosen monomial order.
4. Extract the elimination ideal:

$$I_m = I \cap k[x_1, \dots, x_n],$$

by selecting the elements of G that do not involve t_1, \dots, t_m .

5. The variety $V(I_m)$, defined by the elimination ideal I_m , is the smallest variety in k^n containing the image of the parametrization $F(k^m)$.

We have a similar result for rational parametrizations.

Theorem 3.2 (Rational Implicitization). *If k is an infinite field, let $F : k^m \setminus W \rightarrow k^n$ be the function determined by the rational parametrization (??). Let J be the ideal*

$$J = \langle g_1x_1 - f_1, \dots, g_nx_n - f_n, 1 - gy \rangle \subseteq k[y, t_1, \dots, t_m, x_1, \dots, x_n],$$

where $g = g_1 \cdot g_2 \cdots g_n$ and $W = V(g)$. Also let $J_{1+m} = J \cap k[x_1, \dots, x_n]$ be the $(1 + m)$ -th elimination ideal. Then $V(J_{1+m})$ is the smallest variety in k^n containing $F(k^m \setminus W)$.

Implicitization Algorithm for Rational Parametrizations 3:

Input: Polynomials $f_1, g_1, \dots, f_n, g_n \in k[t_1, \dots, t_m]$, defining a rational map $x_i = f_i/g_i$ for $1 \leq i \leq n$.

Output: The smallest variety $V(J_{1+m}) \subseteq k^n$ containing the image of the parametrization.

Steps:

1. Introduce a new variable y and define the ideal:

$$J = \langle g_1x_1 - f_1, \dots, g_nx_n - f_n, 1 - gy \rangle,$$

where $g = g_1 \cdots g_n$.

2. Choose a lexicographic monomial order such that:

$$y > t_1 > t_2 > \cdots > t_m > x_1 > x_2 > \cdots > x_n.$$

3. Compute a Gröbner basis G for the ideal J with respect to the chosen monomial order.
4. Extract the elimination ideal:

$$J_{1+m} = J \cap k[x_1, \dots, x_n],$$

by selecting the elements of G that do not involve y, t_1, \dots, t_m .

5. The variety $V(J_{1+m})$, defined by the elimination ideal J_{1+m} , is the smallest variety in k^n containing the parametrization.

Problem 3: Consider the parametric set defined by the equations:

$$x = \frac{2t}{1+u^2+t^2}, \quad y = \frac{2tu}{1+t^2+u^2}, \quad z = \frac{t^2-u^2-1}{1+t^2+u^2}.$$

Find equations for the smallest variety V containing the parametrized set.

Solution. We create a polynomial ring with the variables, the parameters, and one additional parameter v , making sure to put all the parameters first and use the Lex order:

```
R = QQ[u, t, v, x, y, z, MonomialOrder => Lex]
```

Next, we compute a Gröbner basis for the system corresponding to the original equations after clearing denominators, plus one additional equation that guarantees the denominators will be nonzero:

```
gens gb ideal(
  x * (1 + u^2 + t^2) - 2 * t,
  y * (1 + t^2 + u^2) - 2 * t * u,
  z * (1 + t^2 + u^2) - (t^2 - u^2 - 1),
  v * (1 + t^2 + u^2) - 1
)
```

The output is:

$$x^2 + y^2 + z^2 - 1, \quad 2xv + 2zv + x^2v + y^2v + z^2v - 1, \quad 2y + 2zv - t^2x + v - t^2 - x.$$

This Gröbner basis has only one equation without any t, u , or v variables in it. This equation defines the smallest variety containing the parametrized set:

$$\boxed{V(x^2 + y^2 + z^2 - 1)}.$$

3.2 Envelopes

Suppose we have a family of plane curves given by the equation

$$F = (x - t)^2 + (y - t^2)^2 - 4 = 0$$

This is a family of circles centered at (t, t^2) with radius 2. The envelope of this family is the curve that is tangent to each of these circles.

Definition 3.3. The *envelope* of a family of plane curves is the variety defined by the equations

$$F = 0, \quad \frac{\partial F}{\partial t} = 0$$

where F is the equation of the family of curves.

Problem 4: Find an equation for the smallest variety containing the envelope of the family of plane curves given by

$$F = (x - t)^2 - y + t = 0.$$

(Alternate formulation: you may be asked to find the singular points of a variety.)

Solution. The derivative of F with respect to t is:

$$\frac{\partial F}{\partial t} = -2x + 2t + 1.$$

By definition of the envelope, to find the smallest variety containing it, we need to eliminate t from the equations:

$$F = 0, \quad \frac{\partial F}{\partial t} = 0.$$

To do this, we use the polynomial ring with lex order:

```
R = QQ[t, x, y, MonomialOrder => Lex]
```

And then compute a Gröbner basis:

```
gens gb ideal((x - t)^2 - y + t, -2*x + 2*t + 1)
```

The output is:

$$4x - 4y - 1, \quad 4t - 4y + 1.$$

The only element of the Gröbner basis that does not depend on t is:

$$4x - 4y - 1.$$

So the smallest variety containing the envelope is:

$$y = x - \frac{1}{4}.$$

Answer: $y = x - \frac{1}{4}$.

4 Radical ideals

Definition 4.1. Let I be an ideal in a commutative ring R . The *radical* of I , denoted \sqrt{I} , is the set of all elements $r \in R$ such that $r^n \in I$ for some $n \geq 1$. We say that I is a *radical ideal* if $I = \sqrt{I}$.

4.1 Big theorems

Theorem 4.2 (Weak Nullstellensatz). *Let I be an ideal in $k[x_1, \dots, x_n]$. Then $I \subsetneq k[x_1, \dots, x_n]$ if and only if $V(I) \neq \emptyset$.*

Proof. Given $a \in k$ and $f \in k[x_1, \dots, x_n]$, we can consider $\bar{f} = f(x_1, \dots, x_{n-1}, a)$ and the ideal \bar{I} generated by \bar{f} for all $f \in I$. Then one shows that if k is algebraically closed and $I \in k[x_1, \dots, x_n]$ is a proper ideal, then there exists $a \in k$ such that $\bar{I} \neq k[x_1, \dots, x_{n-1}]$. This, by induction implies that we end up with a proper ideal of k after restricting finite number of times, and therefore is equal to $\langle 0 \rangle$. \square

Theorem 4.3 (Hilbert's Nullstellensatz). *If $f, f_1, \dots, f_s \in k[x_1, \dots, x_n]$, then*

$$f \in I(V(f_1, \dots, f_s)) \quad \text{if and only if} \quad f^m \in \langle f_1, \dots, f_s \rangle \quad \text{for some integer } m \geq 1.$$

Proof. Consider the ideal

$$\tilde{I} = \langle f_1, \dots, f_s, 1 - yf \rangle \subseteq k[x_1, \dots, x_n, y],$$

where f, f_1, \dots, f_s are as above. We claim that

$$V(\tilde{I}) = \emptyset.$$

To see this, let $(a_1, \dots, a_n, a_{n+1}) \in k^{n+1}$. Either:

- (a_1, \dots, a_n) is a common zero of f_1, \dots, f_s , or
- (a_1, \dots, a_n) is not a common zero of f_1, \dots, f_s .

In the first case, $f(a_1, \dots, a_n) = 0$, since f vanishes at any common zero of f_1, \dots, f_s . Thus, the polynomial $1 - yf$ takes the value $1 - a_{n+1}f(a_1, \dots, a_n) = 1 \neq 0$ at the point $(a_1, \dots, a_n, a_{n+1})$. In particular, $(a_1, \dots, a_n, a_{n+1}) \notin V(\tilde{I})$. In the second case, for some i , $1 \leq i \leq s$, we must have $f_i(a_1, \dots, a_n) \neq 0$. Thinking of f_i as a function of $n + 1$ variables, which does not depend on the last variable, we again conclude that $(a_1, \dots, a_n, a_{n+1}) \notin V(\tilde{I})$. Now apply the Weak Nullstellensatz to conclude that $1 \in \tilde{I}$.

$$1 = \sum_{i=1}^s p_i(x_1, \dots, x_n, y)f_i + q(x_1, \dots, x_n, y)(1 - yf),$$

for some polynomials $p_i, q \in k[x_1, \dots, x_n, y]$. Now set $y = 1/f(x_1, \dots, x_n)$. Then relation (2) above implies that:

$$1 = \sum_{i=1}^s p_i(x_1, \dots, x_n, 1/f)f_i.$$

Multiply both sides of this equation by a power f^m , where m is chosen sufficiently large to clear all the denominators. This yields:

$$f^m = \sum_{i=1}^s A_i f_i,$$

for some polynomials $A_i \in k[x_1, \dots, x_n]$, which is what we had to show. \square

Another formulation of the Nullstellensatz is the following:

Theorem 4.4 (Nullstellensatz). *Let I be an ideal in $k[x_1, \dots, x_n]$. Then $I(V(I)) = \sqrt{I}$.*

In particular, there is a one-to-one correspondence between radical ideals and algebraic sets.

Remark 4.5. *There are a number of questions one can ask about computations for radical ideals. In particular,*

1. *Radical generators: Given an ideal, how can we find a set of generators for the radical of the ideal?*
2. *Radical ideal: Given a set of generators for an ideal, how can we determine if the ideal is radical?*
3. *Radical membership: Given a radical ideal, how can we determine if a given polynomial is in the ideal?*

These answers are all known, but only the last one is in the scope of this course. Deeper theory about saturation and primary decomposition is required.

4.2 Radical ideal problem

We have the following partial result toward this direction.

Lemma 4.6. *Let $I \subset \mathbb{C}[x_1, \dots, x_n]$ be an ideal such that $V(I)$ is finite. If p_i is the unique generator of $I \cap \mathbb{C}[x_i]$, define \bar{p}_i to be*

$$\bar{p}_i = \frac{p_i}{\gcd(p_i, p'_i)},$$

where p'_i is the x_i -derivative of p_i . Then

$$\sqrt{I} = I + \langle \bar{p}_1, \dots, \bar{p}_n \rangle.$$

4.3 Radical membership problem

The radical membership test follows from the Hilbert Nullstellensatz.

Proposition 4.7 (Radical Membership). *Let $I = \langle f_1, \dots, f_s \rangle \subseteq k[x_1, \dots, x_n]$ be an ideal. Then $f \in \sqrt{I}$ if and only if the constant polynomial 1 belongs to the ideal*

$$\tilde{I} = \langle f_1, \dots, f_s, 1 - yf \rangle \subseteq k[x_1, \dots, x_n, y],$$

in which case $\tilde{I} = k[x_1, \dots, x_n, y]$.

Radical Membership Test 4:

Input: An ideal $I = \langle f_1, \dots, f_s \rangle \subseteq k[x_1, \dots, x_n]$ and a polynomial $f \in k[x_1, \dots, x_n]$.

Output: Determine whether $f \in \sqrt{I}$ (i.e., whether $f^m \in I$ for some $m \geq 1$).

Steps:

1. Extend the ring $k[x_1, \dots, x_n]$ by adding a new variable y .
2. Define the ideal:
$$\tilde{I} = \langle f_1, \dots, f_s, 1 - yf \rangle \subseteq k[x_1, \dots, x_n, y].$$
3. Compute a Gröbner basis G for \tilde{I} with respect to a lexicographic order where y is greater than all x_i (i.e., $y > x_1 > x_2 > \dots > x_n$).
4. Check if 1 is in the Gröbner basis G :
 - If $1 \in G$, then $f \in \sqrt{I}$.
 - Otherwise, $f \notin \sqrt{I}$.

Problem 5: Is $x^{11} - x$ in the radical of the ideal $I = \langle xy^3 - x^2, x^3y^2 - y \rangle$?

Solution. We create a polynomial ring with an extra variable t :

$$R = \mathbb{Q}\mathbb{Q}[x, y, z, t]$$

Then we compute a Gröbner basis for the ideal generated by I , plus an additional equation:

$$G = \text{gens gb ideal}(x*y^3 - x^2, x^3*y^2 - y, (x^{11} - x)*t - 1)$$

The output of this computation shows that the answer is (1). This means that the ideal is the whole polynomial ring, and therefore $x^{11} - x$ is in the radical of I .

Answer: Yes.

5 Product and intersection of ideals

- The product of two ideals I and J is the ideal generated by all products of elements of I and J .
- The intersection of two ideals I and J is the ideal generated by all elements that are in both I and J .
- We always have $IJ \subseteq I \cap J$.

Theorem 5.1. Let I, J be ideals in $k[x_1, \dots, x_n]$. Then

$$I \cap J = (tI + (1-t)J) \cap k[x_1, \dots, x_n].$$

Proof. Suppose $f \in I \cap J$. Since $f \in I$, we have $t \cdot f \in tI$. Similarly, $f \in J$ implies $(1-t) \cdot f \in (1-t)J$. Thus, $f = t \cdot f + (1-t) \cdot f \in tI + (1-t)J$. Conversely take $f \in (tI + (1-t)J) \cap k[x_1, \dots, x_n]$. Then $f(x) = g(x, t) + h(x, t)$, where $g(x, t) \in tI$ and $h(x, t) \in (1-t)J$. First, set $t = 0$. Since every element of tI is a multiple of t , we have $g(x, 0) = 0$. Thus, $f(x) = h(x, 0)$ and hence $f(x) \in J$. The same argument above shows that $f(x) \in I$. Therefore, $f \in I \cap J$, and this completes the proof. \square

Algorithm for Computing Intersections of Ideals 5:

Input: Ideals $I = \langle f_1, \dots, f_r \rangle$ and $J = \langle g_1, \dots, g_s \rangle$ in $k[x_1, \dots, x_n]$.

Output: A Gröbner basis of $I \cap J$.

Steps:

1. Define the ideal:

$$K = \langle tf_1, \dots, tf_r, (1-t)g_1, \dots, (1-t)g_s \rangle \subseteq k[x_1, \dots, x_n, t],$$

where t is an auxiliary variable.

2. Choose a lexicographic monomial order such that:

$$t > x_1 > x_2 > \dots > x_n.$$

3. Compute a Gröbner basis G for the ideal K with respect to the chosen monomial order.
4. Extract the elements of G that do not involve the variable t . These elements will form a Gröbner basis for $I \cap J$.
5. Return the Gröbner basis of $I \cap J$.

Problem 6: Define polynomials $f = x^2y$ and $g = xy^2$. Compute:

- (a) The ideal $\langle f \rangle \cap \langle g \rangle$.
- (b) The least common multiple of f and g .
- (c) The greatest common divisor of f and g .

Solution. The intersection will be the first elimination ideal of $\langle tf, (1-t)g \rangle$, where the variable t is greatest. We compute a Gröbner basis:

```
R = QQ[t, x, y, MonomialOrder => Lex]
gens gb ideal (t*x^2*y, (1-t)*x*y^2)
```

The output is:

$$x^2y^2, \quad txy^2 - x^2y^2, \quad tx^2y^2.$$

The only term of the answer that does not depend on t is x^2y^2 . Therefore:

- The intersection of $\langle f \rangle$ and $\langle g \rangle$ is $\langle x^2y^2 \rangle$.
- The least common multiple (LCM) is the generator of the intersection of $\langle f \rangle$ and $\langle g \rangle$, so the LCM is x^2y^2 .
- The greatest common divisor (GCD) is the product of the two polynomials, divided by the LCM, so the GCD is xy .

6 Graph algorithms and integer programming

6.1 Chromatic number

Theorem 6.1. Let G be a graph with n vertices, let $f_G \in \mathbb{C}[x_1, \dots, x_n]$ be the graph polynomial

$$f_G = \prod_{(i,j) \in E} (x_i - x_j),$$

and let

$$I_k = \langle x_1^k - 1, \dots, x_n^k - 1 \rangle.$$

Then G is k -colorable if and only if $f_G \notin I_k$.

Proof. If $f_G \notin I_k$, that means there is an assignment of k -th roots of unity to x_1, x_2, \dots, x_n such that no edge $(i, j) \in E$ has $x_i = x_j$. Thus, G is k -colorable. Conversely, if G is k -colorable, then there is an assignment of k -th roots of unity to x_1, x_2, \dots, x_n such that no edge $(i, j) \in E$ has $x_i = x_j$. Thus, $f_G \notin I_k$. \square

Problem 7: Let G be a graph with n vertices, let $f_G \in \mathbb{C}[x_1, \dots, x_n]$ be the graph polynomial, and let

$$I_k = \langle x_1^k - 1, \dots, x_n^k - 1 \rangle.$$

1. Show that the number of ways to color G with k colors, where two vertices of the same color **ARE allowed** to be adjacent, is equal to the number of points in $V(I)$, and that this number is equal to n^k .
2. Show that the number of ways to color G with k colors, where two vertices of the same color **ARE NOT allowed** to be adjacent, is equal to the number of points in:

$$V(I + \langle f_G \cdot t - 1 \rangle) \quad \text{in } \mathbb{A}_{\mathbb{C}}^{n+1}.$$

Solution. 1. Both sets correspond to picking a root of unity freely at each vertex, there are n^k such many ways.

2. Combinatorially, this corresponds to picking a root of unity freely at each vertex, and then checking that no two adjacent vertices have the same color. This is equivalent to checking that $f_G \cdot t - 1$ is not in I_k . Thus, the number of ways to color G with k colors is the number of points in $V(I + \langle f_G \cdot t - 1 \rangle)$.

6.2 Minimal vertex cover

Problem 8: Let G be a graph and let J be its cover ideal. That is

$$J = \bigcap_{\{i,j\} \in E} \langle x_i, x_j \rangle.$$

1. Show that J is a monomial ideal and its generators are in bijection with vertex covers.
2. Use the method in part (1) to find all the vertex covers of the Moser spindle (the graph in A27). Use Macaulay2 for all computer algebra computations.

Solution. 1. J is the intersection of a bunch of monomial ideals. To show that its generators are in bijection with vertex covers, we note that the generators of J are the monomials corresponding to the vertices in the vertex cover. In particular, each edge $\{x_i, x_j\}$ requires at least one of x_i or x_j to be in a vertex cover.

- The ideal $\langle x_i, x_j \rangle$ corresponds to this requirement: one of these two variables must be in the vertex cover.
 - Taking the intersection over all edges ensures that all edges are covered, giving the cover ideal.
2. We find that the vertex covers of the Moser spindle are as follows. The ideal in question can be generated by the following monomials:

$$\langle x_2x_4x_6x_7, x_1x_3x_5x_7, x_1x_2x_4x_6, x_2x_3x_4x_5x_7, x_1x_3x_4x_5x_6 \rangle$$

so there are 5 vertex covers corresponding to the generators of the ideal.

Problem 9: Consider the pentagon graph with only the boundary edges. Find the minimal vertex covers of this graph. Find the maximal independent sets of this graph (recall that the complement of an independent set is a vertex cover and vice versa).

Solution. We create a polynomial ring with one variable for each vertex:

$$R = \mathbb{Q}[a, b, c, d, e]$$

Then, we create the cover ideal by intersecting the ideals corresponding to each edge and compute a Gröbner basis:

$$J = \text{intersect}(\text{ideal}(a, b), \text{ideal}(b, c), \text{ideal}(c, d), \text{ideal}(d, e), \text{ideal}(e, a)).$$

The Gröbner basis computation is performed using the following Macaulay2 code:

```
R = QQ[a, b, c, d, e]
J = intersect(ideal(a, b), ideal(b, c), ideal(c, d),
ideal(d, e), ideal(e, a))
gens gb J
```

The output of the Gröbner basis computation is:

$$\text{gens gb } J = \{b \cdot d \cdot e, b \cdot c \cdot e, a \cdot c \cdot e, a \cdot c \cdot d, a \cdot b \cdot d\}.$$

Thus, there are five minimal vertex covers:

$$\text{ANSWER: } \{b, d, e\}, \{b, c, e\}, \{a, c, e\}, \{a, c, d\}, \{a, b, d\}.$$

Problem 10: A summer camp hires instructors. Each class needs both instructors present to run. For each of the following questions, explain how the answer is either the chromatic number, the size of a minimal vertex cover, or the size of a maximal independent set in an appropriate graph.

1. Safety regulations prohibit any instructor from teaching more than one class at the camp (due to fatigue). What is the maximal number of classes the camp can offer?
2. Regulations change and instructors are allowed to teach any number of classes. Given that no instructor can teach two different classes at the same time, what is the minimum number of time slots needed for the camp to offer all six classes?
3. The camp wants to distribute radios to a subset of the instructors so that each class will have at least one radio present (in case there is a need for emergency communications). What is the minimum number of radios needed?

Solution. 1. Let G be the graph with vertices corresponding to valid instructor-class pairs, and edges corresponding to pairs with the same instructor or same class. Then the chromatic number of G is the maximal number of classes the camp can offer.

2. Let H be the graph with vertices corresponding to classes and instructors, with edges corresponding to valid instructor-class pairs. Then the size of a minimal vertex cover of H is the minimum number of time slots needed for the camp to offer all six classes.
3. Let G as above. A maximum independent set of G corresponds to a set of instructor-class pairs such that no two pairs share an instructor or class. The size of a maximal independent set of G is the minimum number of radios needed.

6.3 Integer programming

Problem 11: Compute the number of solutions to the following integer programming feasibility problem:

$$\begin{aligned}x_1 + x_2 + x_3 + x_5 + 2x_6 &= 2, \\x_2 + x_4 + x_7 &= 1, \\x_3 + x_4 + x_8 &= 1, \\x_i &\in \{0, 1\}, \quad i = 1, \dots, 8.\end{aligned}$$

Solution. We apply Proposition 7 on p.253 of Cox-Little-O'Shea to the ideal

$$\begin{aligned}f_1 &= x_1 + x_2 + x_3 + x_5 + 2x_6 - 2, \\f_2 &= x_2 + x_4 + x_7 - 1, \\f_3 &= x_3 + x_4 + x_8 - 1, \\g_1 &= x_1^2 - x_1, \\g_2 &= x_2^2 - x_2, \\J = \langle f_i, g_j \rangle_{i=1,\dots,3, j=1,\dots,8} \quad &\text{with} \quad g_3 = x_3^2 - x_3, \\g_4 &= x_4^2 - x_4, \\g_5 &= x_5^2 - x_5, \\g_6 &= x_6^2 - x_6, \\g_7 &= x_7^2 - x_7, \\g_8 &= x_8^2 - x_8.\end{aligned}$$

which will give us the number of complex solutions. However, all the complex solutions will be real in this case because $x_i \in \{0, 1\}$ for $i = 1, \dots, 8$. Thus, we can count the number of real solutions to the integer programming feasibility problem by counting the number of complex solutions to the ideal J . We count that the answer is 16.

Problem 12: Consider the integer programming problem:

$$\text{maximize } x_1 + x_2 + x_3$$

subject to:

$$\begin{aligned}x_1 + 2x_2 + 4x_3 &= 8, \\3x_1 + 7x_2 + x_3 &= 14.\end{aligned}$$

- (1) Use Macaulay2 to show that this problem has no solution when $x_i \in \{0, 1\}$ for $i = 1, 2, 3$.
- (2) Use Macaulay2 to solve the integer programming problem with the constraints $x_i \geq 0$ (but we no longer require $x_i \in \{0, 1\}$). Use the method of replacing constraints of the form $x(x-1)$ by constraints of the form $x(x-1)(x-2)\dots(x-n)$.

- (3) Use Macaulay2 to solve the integer programming problem with the constraints $x_i \geq 0$ (but we no longer require $x_i \in \{0, 1\}$). Use the method of introducing extra variables and representing each x_i in binary form.
- (4) Use Macaulay2 to solve the integer programming problem:

$$\text{maximize } x_1 + x_2 + x_3$$

subject to:

$$\begin{aligned} x_1 + 2x_2 + 4x_3 &= 8, \\ 3x_1 + 7x_2 + x_3 &\leq 14, \\ x_i &\geq 0, \quad i = 1, 2, 3. \end{aligned}$$

Solution. 1. We have the following Macaulay2 code:

```
R = QQ[x1, x2, x3, MonomialOrder => Lex]
I = ideal(x1 + 2*x2 + 4*x3 - 8, 3*x1 + 7*x2 + x3 - 14,
x1^2 - x1, x2^2 - x2, x3^2 - x3)
isEmpty = (I == ideal(1))
```

and we find that `isEmpty` is `true`.

2. We have the following Macaulay2 code:

```
-- Define the polynomial ring with variables x1, x2, x3
R = QQ[x1, x2, x3, MonomialOrder => Lex]

-- Define the linear constraints
f1 = x1 + 2*x2 + 4*x3 - 8
f2 = 3*x1 + 7*x2 + x3 - 14

-- Define the polynomial constraints for integer values
p1 = x1 * (x1 - 1) * (x1 - 2) * (x1 - 3) * (x1 - 4)

p2 = x2 * (x2 - 1) * (x2 - 2)

p3 = x3 * (x3 - 1) * (x3 - 2)

-- Create the ideal representing the system of equations
```

```

I = ideal(f1, f2, p1, p2, p3)

-- Decompose the ideal to find all possible solutions
solutions = decompose I

```

and we find that there is one solution (2,1,1).

3. We have the following Macaulay2 code:

```

R = QQ[b10, b11, b20, b21, b30, b31, MonomialOrder => Lex]

x1 = b10 + 2*b11
x2 = b20 + 2*b21
x3 = b30 + 2*b31

f1 = x1 + 2*x2 + 4*x3 - 8
f2 = 3*x1 + 7*x2 + x3 - 14

p1 = b10^2 - b10
p2 = b11^2 - b11
p3 = b20^2 - b20
p4 = b21^2 - b21
p5 = b30^2 - b30
p6 = b31^2 - b31

objective = x1 + x2 + x3

I = ideal(f1, f2, p1, p2, p3, p4, p5, p6)

solutions = decompose I

```

which gives us the optimal solution (2,1,1) with a maximum value of 4.

4. We have the following Macaulay2 code:

```

R = QQ[x1, x2, x3, s, MonomialOrder => Lex]

-- Define the constraints
f1 = x1 + 2*x2 + 4*x3 - 8
f2 = 3*x1 + 7*x2 + x3 + s - 14

```

```

-- Define polynomial constraints for integer values
p1 = x1 * (x1 - 1) * (x1 - 2) * (x1 - 3) * (x1 - 4)
p2 = x2 * (x2 - 1) * (x2 - 2)
p3 = x3 * (x3 - 1) * (x3 - 2)
p4 = s * (s - 1)

-- Define the objective function
objective = x1 + x2 + x3

-- Combine all constraints into a single ideal
I = ideal(f1, f2, p1, p2, p3, p4)

-- Decompose the ideal to find all solutions
solutions = decompose I

```

and we find that the optimal solution is $(4, 0, 1)$ with a maximum value of 5.

Problem 13: Solve part 4 of the above problem with a single back substitution.

Solution. We begin by turning the inequality constraint into an equality constraint by introducing a slack variable:

$$3x_1 + 7x_2 + x_3 + s = 14, \quad 0 \leq s \leq 14$$

We will represent the slack variable with binary variables. From the constraint, it is clear that $s \leq 14$, so we can write:

$$s = s_0 + 2s_1 + 4s_2 + 8s_3$$

where each s_i is either 0 or 1. We now have the constraints:

$$x_1 + 2x_2 + 4x_3 = 8$$

$$3x_1 + 7x_2 + x_3 + s_0 + 2s_1 + 4s_2 + 8s_3 = 14$$

Where $x_i \geq 0$ and each x_i is either 0 or 1. From the two constraints, we see that in fact $x_1 = 0, 1, 2, 3$, or 4; $x_2 = 0, 1, 2$; and $x_3 = 0, 1$, or 2.

To solve the problem with a single back substitution, we need to introduce one more variable v equal to the output of the cost function and add this constraint to the ideal. Note that the x and the v come last because we want to get equations with those variables isolated, i.e. we eliminate the s . We have the following Macaulay2 code:

```

R = QQ[s0, s1, s2, s3, x1, x2, x3, v, MonomialOrder => Lex]

I = ideal(x1 + x2 + x3 - v,

```

```

x1 + 2*x2 + 4*x3 - 8,
3*x1 + 7*x2 + x3 + s0 + 2*s1 + 4*s2 + 8*s3 - 14,
x1*(x1-1)*(x1-2)*(x1-3)*(x1-4),
x2*(x2-1)*(x2-2),
x3*(x3-1)*(x3-2),
s0*(s0-1),
s1*(s1-1),
s2*(s2-1),
s3*(s3-1)

```

gens gb I

The Gröbner basis returned is:

$$\begin{aligned}
v^3 - 11v^2 + 38v - 40, \quad 6x^3 - v^2 + 9v - 26, \\
2x^2 + v^2 - 7v + 10, \quad 3x_1 - v^2 + 3v - 2, \\
6s_3 - v^2 + 9v - 20, \quad 6s_2 - v^2 + 9v - 20, \\
s_1, \quad 3s_0 - v^2 + 6v - 8
\end{aligned}$$

We factor the first polynomial:

$$v^3 - 11v^2 + 38v - 40 = (v - 5)(v - 4)(v - 2)$$

The largest root is $v = 5$, so this is the maximum value of the cost function. We can find when it is achieved using back substitution:

$$\begin{aligned}
6x_3 - 25 + 45 - 26 &\implies x_3 = 1 \\
2x_2 + 25 - 35 + 10 &\implies x_2 = 0 \\
3x_1 - 25 + 15 - 2 &\implies x_1 = 4
\end{aligned}$$

Answer: The optimum value 5 of the cost function is achieved when $(x_1, x_2, x_3) = (4, 0, 1)$.

7 Groebner degeneration and flatness

We will now discuss the concept of Groebner degeneration through the lens of flatness with a specific example. **There might be some issues with the general proof.**

Definition 7.1. An S -module M' is **flat** $\otimes_S M'$ is an exact functor on the category of S -modules.

Let $I = \langle xy^3 - x^2, x^3y^2 - y \rangle \subset R = \mathbb{C}[x, y]$. Buchberger's algorithm gives a Groebner basis for the ideal:

$$G = \{x^3y^2 - y, x^4 - y^2, xy^3 - x^2, y^4 - xy\}$$

so that $\text{init } I = \langle x^4, x^3y^2, xy^3, y^4 \rangle$.

Claim 7.2 (Groebner degeneration). *There is a flat family $T \rightarrow \mathbb{A}^1$ with generic fiber isomorphic to $\text{Spec } R/I$ and special fiber isomorphic to $\text{Spec } R/\text{init } I$.*

Lemma 7.3. *An S -module M' is flat if and only if every relation in M' comes from a relation in S . Specifically, if we have*

$$\sum_i s_i m'_i = 0$$

then there exist $n_i \in M'$ and $t_{ij} \in S$ such that

$$\begin{aligned} m'_i &= \sum_j t_{ij} n_j \\ \sum_i s_i t_{ij} &= 0 \end{aligned}$$

Proof. Wikipedia. \square

Consider the map $\mathbb{C}[t] \rightarrow M = \mathbb{C}[x, y, t]/\langle x^4 + tr_1, x^3y^2 + tr_2, xy^3 + tr_3, y^4 + tr_4 \rangle$ where r_i are the non-leading terms in the Groebner basis G . I claim that the Spec of this map is the desired family. It remains to check that M is a flat $\mathbb{C}[t]$ -module.

Theorem 7.4. *Let I be an ideal in $\mathbb{C}[x_1, \dots, x_n]$. Every $f \in \mathbb{C}[x_1, \dots, x_n]$ is congruent modulo I to a unique $r \in \mathbb{C}[x_1, \dots, x_n]$ such that r is a \mathbb{C} -linear combination of monomials not in I . Moreover, the monomials not in $\text{init } I$ are linearly independent modulo I . In particular if we have*

$$\sum_i s_i m_i = 0$$

where m_i are monomials not in $\text{init } I$, then $s_i = 0$.

The problem with the calculation that comes next is that Groebner bases are only about division over \mathbb{C} not over $\mathbb{C}[t]$. I am sure that this is fixable but I am not sure exactly how I should fiddle with the argument.

Corollary 7.5. *The monomials not in $\text{init } I$ form a \mathbb{C} -basis for $\mathbb{C}[x_1, \dots, x_n]/I$.*

Now we will finish by checking that M is a flat $\mathbb{C}[t]$ -module. Suppose we have a nontrivial relation in M :

$$\sum_i s_i(t) m_i(x, y, t) \in \langle x^4 + tr_1, x^3y^2 + tr_2, xy^3 + tr_3, y^4 + tr_4 \rangle$$

where the s_i are in $\mathbb{C}[t]$ and the $m_i \in M$. By Theorem 1.4 we can write each m_i as a \mathbb{C} -linear combination of monomials n_j not in $\text{init } I$.

$$m_i = \sum_j t_{ij} n_j(x, y, z)$$

where the t_{ij} are in \mathbb{C} . Then we plug back in and we see that

$$\sum_j \left(\sum_i s_i(t) t_{ij} \right) n_j(x, y, t) \in \langle x^4 + tr_1, x^3 y^2 + tr_2, xy^3 + tr_3, y^4 + tr_4 \rangle$$

but recall that the n_j are linearly independent modulo I so we must have all the coefficients are zero. This is precisely the criterion of flatness.

8 Affine vs. projective flatness

Remark 8.1. *If the total space of a family $T \rightarrow \mathbb{A}^1$ is projective, then one can check flatness by checking that the fibers have the same Hilbert polynomial.*

Is this fact related to Groebner degenerations?

Definition 8.2. *Let $I \subset \mathbb{C}[x_1, \dots, x_n]$ be an ideal. The affine Hilbert function of I is the function $s \in \mathbb{N} \mapsto \dim \mathbb{C}[x_1, \dots, x_n]_{\leq s} / I_{\leq s}$ is the number of monomials of degree at most s not in I .*

Proposition 8.3. 1. *The affine Hilbert function h_I^a of I is eventually a polynomial.*

2. *The affine Hilbert polynomial of I is equal to the affine Hilbert polynomial of $\text{init } I$.*

Definition 8.4. *Let $I \subset \mathbb{C}[x_0, \dots, x_n]$ be a homogeneous ideal. The Hilbert function of I is the function $s \mapsto \dim \mathbb{C}[x_0, \dots, x_n]_s / I_s$.*

Proposition 8.5. 1. *The Hilbert function h_I of I is eventually a polynomial.*

2. *The Hilbert polynomial of I is equal to the Hilbert polynomial of $\text{init } I$.*

3. $h_I(s) = h_I^a(s) - h_I^a(s-1)$.

4. $h_I(s) = h_J(s)$ where $J \subset k[x_1, \dots, x_n]$ and $I \subset k[x_0, \dots, x_n]$ is its homogenization with respect to x_0 .

Corollary 8.6. *The dimension of the affine cone over a projective variety is one more than the dimension of the projective variety. The dimension of the projective closure of an affine variety is equal to the dimension of the affine variety.*