Exercises: Computational Commutative Algebra

CIMPA school: Algebraic and Tropical Methods for Solving Differential Equations

Matías Bender
Inria - École polytechnique, France
http://mbender.github.io

June 16, 2023

In what follows, $\mathbb{K}$ denotes a field.

1 Univariate polynomials and resultants

Exercise 1.1 *Given polynomials* $f_1, \dots, f_r \in \mathbb{K}[x]$*, prove that there is a polynomial* $\texttt{GCD}(f_1, \dots, f_r) \in \mathbb{K}[x]$ *such that* $\langle f_1, \dots, f_r \rangle = \langle f \rangle$*.*

$\longrightarrow$ ***Hint****: First, prove the statement for* $r = 2$*. You can use the Euclidean algorithm. Then, prove that* $\texttt{GCD}(f_1, f_2, f_3) = \texttt{GCD}(\texttt{GCD}(f_1, f_2), f_3)$*.*

Exercise 1.2 *Given a polynomial ring* R*, e.g.* $R = \mathbb{C}[y]$*, prove that there are two polynomials* $A, B \in R[x]$ *such that* $\texttt{Res}(f, g, x) = A\, g + B\, f$ *such that* $\texttt{deg}_x(A) < \texttt{deg}_x(g)$ *and* $\texttt{deg}_x(B) < \texttt{deg}_x(f)$*.*

$\longrightarrow$ ***Hint****: Consider the adjugate of the Sylvester matrix.*

Exercise 1.3 *Let* $f := \sum_{i=0}^{n} f_i(y)\, x^i, g := \sum_{i=0}^{m} g_i(y)\, x^i \in \mathbb{K}[x, y]$*. Let* $p_y \in \mathbb{C}$ *such that* $f_n(p_y) \neq 0$*. Then,*

$$\texttt{Res}(f, g, x) \mid_{y=p_y} = f_n(p_y)^k \, \texttt{Res}(f(x, p_y), g(x, p_y), x),$$

where $k = m - \texttt{deg}_x(g(x, p_y))$*.*

$\longrightarrow$ **Hint**: Consider the Sylvester matrix of (f, g) and evaluate it at $y = p_y$. Compare this matrix to the Sylvester matrix of $(f(x, p_y), g(x, p_y))$.

Exercise 1.4 (Extension theorem in two variables) *Given* f, g *as before and* $p_y \in \mathbb{C}$ *such that* $f_n(p_y) \neq 0$ *or* $g_m(p_y) \neq 0$*, then there is* $p_x \in \mathbb{C}$ *such that* $f(p_x, p_y) = g(p_x, p_y) = 0$*.*

$\longrightarrow$ ***Hint****: Recall that* $\texttt{Res}(f(x, p_y), g(x, p_y), x) = 0$ *if and only if* $\texttt{deg}_x(\texttt{GCD}(f(x, p_y), g(x, p_y))) \geq 1$*.*

Exercise 1.5 *Show that, if* $\texttt{GCD}(f_n, g_m) \neq 1$*, then every root* $p_y \in \mathbb{C}$ *of* $\texttt{Res}(f, g, x)$ *can be extended to a solution* $(p_x, p_y) \in \mathbb{C}^2$ *such that* $f(p_x, p_y) = g(p_x, p_y) = 0$*.*

1.1 Homogeneous resultants

Definition 1 *Given* $f := \sum_{i=0}^{n} f_i(y)\, x^i \in \mathbb{C}[x, y]$*, we define its* homogenization *as the polynomial* $f^h := \sum_{i=0}^{n} f_i(y)\, x_0^{n-i}\, x_1^i \in \mathbb{C}[x_0, x_1, y]$*. Observe that every monomial in* f^h *has degree* n *with respect to the block of variables* $\{x_0, x_1\}$*, so we say it is* homogeneous *with respect to this blocks of variables.*

Exercise 1.6 *Prove that, for any* $\lambda \in \mathbb{C} \setminus \{0\}$*,* $f^h(\lambda, \lambda\, x, y) = \lambda^n\, f(x, y)$*. What is* $f^h(0, x, y)$*?*

Exercise 1.7 *Prove that, given $f \in \mathbb{C}[x,y]$ and $(p_{x,0}, p_{x,1}, p_y) \in \mathbb{C}^3$, for any $\lambda \in \mathbb{C} \setminus \{0\}$, we have that $f^h(\lambda\, p_{x,0}, \lambda\, p_{x,1}, p_y) = \lambda^n\, f^h(p_{x,0}, p_{x,1}, p_y)$. In particular, if $f^h(p_{x,0}, p_{x,1}, p_y) = 0$, then $f^h(\lambda\, p_{x,0}, \lambda\, p_{x,1}, p_y) = 0$, for any non-zero λ.*

The previous exercise tell us that we can think the zero set of f^h as belonging to $\mathbb{P}^1 \times \mathbb{C}^1$.

Exercise 1.8 *Consider two bivariate polynomials $f := \sum_{i=0}^n f_i(y)\, x^i, g := \sum_{i=0}^m g_i(y)\, x^i \in \mathbb{C}[x,y]$. Let $p_y \in \mathbb{C}$. Prove that $\texttt{Res}(f,g,x)|_{y=p_y} = 0$ if and only if there is a non-zero pair $(p_{x,0}, p_{x,1}) \in \mathbb{C}^2 \setminus \{(0,0)\}$ such that $f^h(p_{x,0}, p_{x,1}, p_y) = g^h(p_{x,0}, p_{x,1}, p_y) = 0$.*

$\longrightarrow$ **Hint**: Split you analysis in two cases, one when $x_0 \neq 0$ and other when $x_0 = 0$. Use the extension theorem (exercise 1.4).

Definition 2 (Resultant of binary form) *Consider the polynomial ring $R = \mathbb{Z}[\bar{f}_0, \dots, \bar{f}_n, \bar{g}_0, \dots, \bar{g}_m]$, where $\bar{f}_0, \dots, \bar{f}_n, \bar{g}_0, \dots, \bar{g}_m$ are new variables. Define $\bar{f} := \sum_{i=0}^n \bar{f}_i x_0^{n-i}\, x_1^i \in R[x_0, x_1]$ and $\bar{g} := \sum_{i=0}^m \bar{g}_i x_0^{m-i}\, x_1^i \in R[x_0, x_1]$ and consider the Sylvester matrix $\texttt{Sylv}$ associated to $\bar{f}\ |_{x_0=1}$ and $\bar{g}\ |_{x_0=1}$ in $R^{(n+m)\times(n+m)}$. The resultant $\texttt{Res}_{n,m} \in R$ of two binary forms of degrees n and m is the determinant of the matrix $\texttt{Sylv} \in R^{(n+m)\times(n+m)}$.*

Given $F \in R$ and $f, g \in \mathbb{C}[x_0, x_1]$ binary forms of degrees n and m, we define

$$F(f,g) := F|_{\{\bar{f}_i = f_i\}_{i \le n}, \{\bar{g}_j = g_j\}_{j \le m}} \,.$$

Exercise 1.9 *Given two binary forms $f := \sum_{i=0}^n f_i x_0^{n-i}\, x_1^i \in \mathbb{C}[x_0, x_1]$ and $g := \sum_{i=0}^m g_i x_0^{m-i}\, x_1^i \in \mathbb{C}[x_0, x_1]$, show that there is $(p_0, p_1) \in \mathbb{C}^2 \setminus \{(0,0)\}$ such that $f(p_0, p_1) = g(p_0, p_1) = 0$ if and only if the matrix $\texttt{Res}_{n,m}(f,g) = 0$.*

$\longrightarrow$ **Hint**: Use a similar argument as in Exercise 1.8

Warning: *To solve the following exercise, you might need to use some tools from algebraic geometry that goes beyond this course, as properties of projective varieties and fibers of polynomial maps.*

Exercise 1.10 *Let $n, m \geq 1$. Consider the incidence variety*

$$\Omega = \{((f_0, \dots, f_n), (g_0, \dots, g_m), (p_0, p_1)) \in \mathbb{P}^n \times \mathbb{P}^m \times \mathbb{P}^1 : \sum_{i=0}^n f_i p_0^{n-i} p_i = \sum_{i=0}^m g_i p_0^{m-i} p_i = 0\}.$$

Let $\pi : \mathbb{P}^n \times \mathbb{P}^m \times \mathbb{P}^1 \to \mathbb{P}^n \times \mathbb{P}^m$ be the projection into the first two components.

- *Show that $\pi(\Omega)$ is a hyperplane in $\mathbb{P}^n \times \mathbb{P}^m$.*
- *Show that this hyperplane is defined by a principal ideal given by $\langle \texttt{Res}_{n,m} \rangle$.*
- *Prove that $\texttt{Res}_{n,m}$ is irreducible.*

$\longrightarrow$ **Hint**: See [Stu02, Thm. 4.4]

Indeed, we can generalize this ideas to systems of $s+1$ homogeneous polynomial equations in $\mathbb{C}[x_0, \dots, x_s]$. The interested reader can find a great introduction to the subject in [Stu02, Chp. 4] and [CLO05, Chp. 3]. These ideas were generalised to sparse polynomial systems; see [CLO05, Chp. 7] for an didactical introduction to the subject, or [GKZ94] for a complete, but highly technical, treatment.

2 Ideals and varieties

In this section, let $R := \mathbb{C}[x_1, \dots, x_n]$.

Exercise 2.1 *Using the Noetherian property of R, that is, that every ideal in R is finitely generated, show that R satisfies the ascending chain condition, that is, if we have a sequence of ideals*

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

then there is k_0 such that, for every $k > k_0$, $I_{k_0} = I_k$.

$\longrightarrow$ **Hint**: Prove that $\bigcup_{i=1}^{\infty} I_i$ is an ideal and consider a finite set of generators of this ideal.

Exercise 2.2 *Let I and J be ideals in R. Show the following:*

- $V(I + J) = V(I) \cap V(J)$.
- $V(I \cap J) = V(I) \cup V(J)$.
- $\sqrt{I} \cap \sqrt{J} = \sqrt{I \cap J}$.
- $V(I) = V(\sqrt{I})$.

Exercise 2.3 *Let V and W be subvariaties of $\mathbb{C}^n$. Show the following:*

- $I(V \cap W) = \sqrt{I(V) + I(W)}$
- $I(V \cup W) = I(V) \cap I(W)$

Exercise 2.4 (Rabinowitsch trick) *Use the weak version of Hilbert's Nullstellenstatz, i.e., if $V(I)$ then $1 \in I$, to prove its strong version, i.e., if $(\forall p \in V(I))g(p) = 0$ then $g \in \sqrt{I}$.*

$\longrightarrow$ **Hint**: Using the radical membership algorithm introduced in the lecture, prove that, if g vanishes at every point in $V(f_1, \dots, f_r)$, there are $q_0, q_1, \dots, q_r \in R[t]$ such that $1 = q_0\,(g\,t - 1) + \sum_i q_i\, f_i$. What happens is you replace (symbolically) t by $\frac{1}{g}$ and clear denominators?

3 Gröbner bases

In this section, let $R := \mathbb{C}[x_1, \dots, x_n]$.

Definition 3 (Graded reverse lexicographical order) *We define the* graded reverse lexicographical order $>_{grevlex}$ *as a monomial ordering such that, given $x^\alpha, x^\beta \in R$, $x^\alpha >_{grevlex} x^\beta$ if*

- $\mathtt{deg}(x^\alpha) > \mathtt{deg}(x^\beta)$, *or*
- $\mathtt{deg}(x^\alpha) = \mathtt{deg}(x^\beta)$ *and there is $k \leq n$ such that,*
  - $\alpha_i = \beta_i$, *for every $i > k$ and*
  - $\alpha_k < \beta_k$.

Example 1 *The monomial $x_1^2\, x_2^2\, x_3^2 >_{grevlex} x_1^2\, x_2^3$ because the degree of the right hand side is bigger than the one in the left hand side, but $x_1^2\, x_2^2\, x_3^2 <_{grevlex} x_1^2\, x_2^3\, x_3$ because the degree with respect to x_3 in the right hand side is smaller than the one in the left hand side.*

Exercise 3.1 *Prove that $<_{grevlex}$ is a monomial ordering.*

Exercise 3.2 *Present an example that illustrates that the graded reverse lexicographical order $<_{grevlex}$ and the graded lexicographical order $<_{glex}$ are different.*

Exercise 3.3 *Show that in the ring of univariate polynomials $\mathbb{C}[x]$, there is a unique monomial ordering. How does this order looks like?*

$\longrightarrow$ **Hint**: Revise the definition of monomial ordering.

Exercise 3.4 *Given $f, g \in R$, show that, if $g \in \langle f \rangle$, then $\mathrm{LM}_>(f)|\mathrm{LM}_>(g)$, for any monomial ordering $>$. Conclude that $g \in \langle f \rangle$ if and only if $\textsc{Rem}(g, f, <) = 0$, for any monomial ordering.*

Exercise 3.5 *Given $f_1, \ldots, f_r, g \in R$ and a monomial ordering $>$, prove that*

$$g - \textsc{Rem}(g, [f_1, \ldots, f_r], >) \in \langle f_1, \ldots, f_r \rangle.$$

Conclude that, if $\textsc{Rem}(g, [f_1, \ldots, f_r], >) = 0$, then $g \in \langle f_1, \ldots, f_r \rangle$. Prove that the opposite implication does not hold for arbitrary $f_1, \ldots, f_r, g \in R$.

Exercise 3.6 *Prove that, for any monomial ordering $>$, every ideal I has a finite Gröbner basis.*

⟶ **Hint**: Remember that the ring R satisfies the ascending chain condition, see exercise 2.1. Use this property on a chain of ideals generated increasingly by adding leading monomials of polynomials in I.

3.1 Gröbner bases of special systems

Exercise 3.7 (Gröbner bases of univariate polynomials) *Given polynomials $f_1, \ldots, f_r \in \mathbb{C}[x]$, prove that $\{\mathtt{GCD}(f_1, \ldots, f_r)\}$ is a Gröbner bases of $\langle f_1, \ldots, f_r \rangle$, for any monomial ordering.*

Exercise 3.8 (Gröbner bases of empty systems) *Let G be a Gröbner basis of I with respect to a monomial ordering $<$. Show that $V(I) = \emptyset$ if and only if there is $c \in \mathbb{C}$ such that $c \in G$.*

Definition 4 *A* monomial ideal *is an ideal generated by monomials. Given an ideal I and a monomial ordering $>$, we define the monomial ideal of I as $\mathrm{LM}_>(I) := \langle \mathrm{LM}_<(f) : f \in I \rangle$.*

Exercise 3.9 (Gröbner bases of monomial ideals) *Prove that G is a Gröbner basis of I with respect to $>$ if and only if*

$$\langle \mathrm{LM}_>(g) : g \in G \rangle = \mathrm{LM}_>(I).$$

Exercise 3.10 *Prove that if I is a monomial ideal and $f \in I$, then $\textsc{Supp}(f) \subset I$, that is, every monomial appearing in f belongs to I.*

Exercise 3.11 *Prove that if I is a monomial ideal, then any generating set of I is a Gröbner basis of I with respect to any monomial ordering.*

Exercise 3.12 (Gröbner bases of linear systems) *Given linear polynomials $f_1, \ldots, f_r$ and a monomial ordering $>$ such that $x_1 > x_2 > \cdots > x_n$, what is the Gröbner basis of $\langle f_1, \ldots, f_r \rangle$?*

⟶ **Hint**: Consider the linear polynomials in $\langle f_1, \ldots, f_r \rangle$. What are the leading monomials of these linear polynomials?

3.2 Uniqueness of Gröbner bases

Definition 5 *We say that a Gröbner basis G with respect to $<$ of I is* minimal *if we can not remove an element $f \in G$ in such a way that $G \setminus \{f\}$ is still a Gröbner basis of I with respect to $<$.*

We say G is reduced *if, for every $f \in G$, the leading coefficient of f is one, i.e. $\mathrm{LC}_>(f) = 1$, and there is no element $\bar{f} \in G \setminus f$ such that $LM(\bar{f})$ divides a monomial in $\textsc{Supp}(f)$.*

Exercise 3.13 *Prove that, for a given monomial ordering, each ideal has a unique minimal reduced Gröbner basis.*

3.3 Computing Gröbner bases - Buchberger algorithm

Definition 6 *Given an ideal I, a monomial ordering $>$, and a finite subset $\{f_1, \ldots, f_r\} \subset I$, we say that $g \in I$ has a* standard representation *if there are $h_1, \ldots, h_r \in \mathbb{C}[x_1, \ldots, x_n]$ such that we can write $g = \sum h_i\, f_i$ and $\mathrm{LM}_>(g) \geq \mathrm{LM}_>(h_i\, f_i)$, for every i.*

Exercise 3.14 *Prove that if $\textsc{Rem}(g, [f_1, \ldots, f_r], >) = 0$, then there is a standard representation for g. Construct an example where the opposite does not hold.*

$\longrightarrow$ **Hint**: Consider the polynomials $(q_1, \ldots, q_r)$ constructed via the division algorithm when $[f_1, \ldots, f_r]$ is not a Gröbner basis.

Exercise 3.15 *Prove that if, for every $g \in I$ we can find a standard representation using $\{f_1, \ldots, f_r\}$, then $\{f_1, \ldots, f_r\}$ is a Gröbner basis of I with respect to $>$.*

Definition 7 *Given $f, g \in \mathbb{C}[x_1, \ldots, x_n]$ and a monomial order $>$, we define its S-polynomial as*

$$S_>(f, g) = \frac{LT(g)}{\mathtt{GCD}(LM(f), LM(g))}\, f - \frac{LT(f)}{LM(f), LM(g)}\, g$$

Where $\mathtt{GCD}(x^\alpha, x^\beta) = \prod_i x_i^{\min(\alpha_i, \beta_i)}$.

Exercise 3.16 *Prove that, if $x^\alpha\, \mathrm{LM}_>(f) - x^\beta\, \mathrm{LM}_>(g) = 0$, then there is a monomial x^γ such that $\frac{LT(g) \cdot x^\gamma}{GCD(LM(f), LM(g))} = x^\alpha$ and $\frac{LT(f) \cdot x^\gamma}{GCD(LM(f), LM(g))} = x^\beta$.*

Exercise 3.17 *Prove that, if $h = c_\alpha\, x^\alpha\, f + c_\beta\, x^\beta\, g$ is such that $\mathrm{LM}(h) < LM(x^\alpha\, f)$ and $LM(x^\alpha\, f) = LM(x^\beta\, g)$, then $S_>(f, g)$ divides h.*

Exercise 3.18 *Prove that if $h = \sum_{i=1}^r c_{\alpha_i} x^{\alpha_i} f_i$ such that, for every pair (i, j), $LM(x^{\alpha_i}\, f_i) = LM(x^{\alpha_j}\, f_j)$ and $LM(x^{\alpha_i}\, f_i) > LM(h)$, then we can find monomials $x^{\beta_{i,j}}$ and constants $c_{\beta_{i,j}}$ such that $h = \sum_{i,j} c_{\beta_{i,j}}\, x^{\beta i,j}\, S_>(f_i, f_j)$ and, for each pair (i, j), $LM(x^{\beta_{i,j}}\, S_>(f_i, f_j)) < LM(x^{\alpha_i}\, f_i)$*

Exercise 3.19 *Consider $h = \sum_i g_i\, f_i$ and let x^δ be the maximal possible monomial with respect to $>$ among the summands $LM(g_i\, f_i)$. Prove that, if $LM(h) < x^\delta$, there are polynomials $\{\bar{g}_i\}_i, \{\bar{g}_{i,j}\}_{i,j}$ such that $\mathrm{LM}_>(\bar{g}_i f_i) < x^\delta$, for every i, $\mathrm{LM}_>(\bar{g}_{i,j} S_>(f_i, f_j)) < x^\delta$, for every pair i, j, and*

$$h = \sum_i \bar{g}_i\, f_i + \sum_{i,j} \bar{g}_{i,j}\, S_>(f_i, f_j).$$

$\longrightarrow$ **Hint**: Split the polynomials g_i as $LT(g_i) + (g - LT(g_i))$ and observe that $\mathrm{LM}((g - LT(g_i))\, f_i) < x^\delta$.

Exercise 3.20 (Buchberger criterion) *Let $f_1, \ldots, f_r$ be such that we can find a standard representation of $S_>(f_i, f_j)$, for each i, j. Then, $\{f_1, \ldots, f_r\}$ is a Gröbner basis of $\langle f_1, \ldots, f_r \rangle$.*

$\longrightarrow$ **Hint**: Given $g \in \langle f_1, \ldots, f_r \rangle$, consider polynomials $h_1, \ldots, h_r$ such that $g = \sum_i h_i\, f_j$ and the maximal $\mathrm{LM}_<(h_i\, f_i)$ with respect to $>$, say x^δ, is minimal among all the ways of writing g as a polynomial combination of $f_1, \ldots, f_r$. Show that in this case the representation has to be standard.

Exercise 3.21 *Prove termination and correctness of Buchberger algorithm.*

$\longrightarrow$ **Hint**: Remember that $\mathbb{C}[x_1, \ldots, x_n]$ satisfies the *ascending chain condition*; see exercise 2.1.

Exercise 3.22 *Consider Buchberger algorithm in the following two cases:*

- *Univariate polynomials, that is, $f_1, \ldots, f_r \in \mathbb{C}[x]$.*

Algorithm 1 `BuchbergerAlgorithm`

```
Require: Polynomials $f_1, \dots, f_r$ and a monomial ordering $>$.
Ensure: A Gröbner basis $G$ of $\langle f_1, \dots, f_r \rangle$ with respect to $<$.
  $G \leftarrow [f_1, \dots, f_r]$
  PAIRS $\leftarrow \{(f_i, f_j) : 1 \leq i < j \leq r\}$
  while PAIRS $\neq \emptyset$ do
    $(f, g) \leftarrow$ Choose pair in PAIRS.
    PAIRS $\leftarrow$ PAIRS $\setminus \{(f, g)\}$.
    $r \leftarrow \textsc{Rem}(S_{>}(f, g), G, >)$
    if $r \neq 0$ then
      PAIRS $\leftarrow$ PAIRS $\cup \{(f, r) : f \in G\}$.
      Add $r$ in the tail of $G$.
    end if
  end while
  return $G$.
```

- *Linear forms, that is, $f_1, \dots, f_r \in \mathbb{C}[x_1, \dots, x_n]$ and each f_i is linear.*

Which classical algorithms allow us to compute Gröbner bases in these cases?

We say that a *reduction to zero* occurs in Buchberger algorithm whenever $r = 0$. In practice, most of the computations are wasted on computing reductions to zero. For this reason, several approaches were developed to avoid them. In what follows, we will prove a criterion by Buchberger to avoid some of these reductions to zero. The interested reader can find an extensive list of criterions in [EF17].

Exercise 3.23 *Consider $\{f_1, \dots, f_r\}$. Consider a pair $(, ij)$ such that* $\texttt{GCD}(\mathrm{LM}(f_1), \mathrm{LM}(f_2)) = 1$. *Then, we can skip the pair (i, j) from Buchberger algorithm.*

$\longrightarrow$ **Hint**: Show that there is a standard representation of $S_{<}(f_i, f_j)$ only involving f_i, f_j. For that, show that, if $x^\alpha < LM(f_j)$ or $x^\beta < LM(f_i)$, then $x^\alpha\, f_i - x^\beta\, f_j$ is a standard representation.

3.4 How hard is to compute Gröbner bases?

The following classical example is due to Masser & Philippon and Lazard & Mora.

Exercise 3.24 *Fix $d \in \mathbb{N}$ and consider the ideal $I := \{f_1, \dots, f_n\} \subset \mathbb{C}[x_1, \dots, x_n]$ defined by the polynomials*

$$\begin{cases} f_1 = x_1^d \\ f_2 = x_1 - x_2^d \\ \quad\vdots \\ f_{n-1} = x_{n-2} - x_{n-1}^d \\ f_n = 1 - x_{n-1}\, x_n^{d-1} \end{cases}$$

- *Show that $V(I) = \emptyset$.*
- *Consider $g_1, \dots, g_n$ such that $1 = \sum_i g_i\, f_i$. Prove that* $\texttt{deg}(g_1) \geq d^{n-1}\,(d-1)$.

  $\longrightarrow$ **Hint**: Consider the previous identity over the parametric curve defined by

  $$t \mapsto \left(t^{d^{n-1}\,(d-1)}, t^{d^{n-2}\,(d-1)}, \dots, t^{d-1}, \frac{1}{t} \right).$$

  Bound the degree of g_1 by studying the degree of t.

Whenever $V(I)$ has a finite number of solutions (or it is empty), roughly speaking, the maximal degree of an element a the Gröbner basis is at most single exponential in the number of variables [Kol88, Jel05]. In the general case, this upper bound is double exponential [MM82].

4 Examples in Singular

Go to `https://www.singular.uni-kl.de`, download, and install the open-source CAS[1] Singular [DGPS22].

Exercise 4.1 *Compute the Gröbner bases of the following ideal with respect to the degree reverse lexicographical and the lexicographical monomial ordering. Which computation was faster? Which Gröbner basis has less elements?*

```
ring r  = 0,(a,b,c,d),dp; // We initialize a ring of charact. zero
                          // with variables (a,b,c,d) and
                          // the monomial ordering grevlex
ideal i = a+b2+c+d,ab2+a2d+bc+cd,a2bc+ab2d+acd+bcd,abc10d-1; // we define the ideal i.
                                                             // Singular's syntax:
                                                             // b2c = b^2*c.
groebner(i); // we compute the GB wrt grevlex

ring s  = 0,(a,b,c,d),lp; // We initialize another ring of char. 0
                          // variables (a,b,c,d) and a lexicographical monomial ordering.
ideal i = imap(r,i); // We recast the ideal i into this ring
groebner(i); // we compute the GB wrt lex
```

5 Polynomial systems with a finite number of solutions

Definition 8 *We say that an ideal I is* zero dimensional *when $V_{\mathbb{C}^n}(I)$ is finite.*

5.1 Properties of zero dimensional systems

Exercise 5.1 *Prove that if the system is zero dimensional, for every $i \in \{1, \ldots, n\}$, there is $g_i(x_i) \in \mathbb{C}[x_i]$ such that $g_i \in I$.*

$\longrightarrow$ **Hint**: Use the fact that, for each i, the possible values for the i-th coordinate of each solution is finite and construct a polynomial that vanishes at these points.

Exercise 5.2 *Prove that, if G is a Gröbner basis of a zero dimensional ideal I with respect to any monomial ordering $>$, for each $i \in \{1, \ldots, n\}$, there is $g_i \in G$ such that $\mathrm{LM}_>(g_i) \in \mathbb{C}[x_i]$.*

Exercise 5.3 *Let I be a zero dimensional ideal. Prove that, if its n-th elimination ideal $I_{n-1} := I \cap \mathbb{C}[x_n]$ is generated by $h_n(x_n)$, i.e., $I_{n-1} = \langle h_n(x_n) \rangle$, then for every $p_n \in \mathbb{C}$ such that $h_n(p_n) = 0$, there are $(p_1, \ldots, p_{n-1}) \in \mathbb{C}^{n-1}$ such that $(p_1, \ldots, p_n) \in V_{\mathbb{C}^n}(I)$.*

$\longrightarrow$ **Hint**: Use the extension theorem (Exercise 6.3) together with Exercise 5.2

Exercise 5.4 *Given $h_1, \ldots, h_r \in \mathbb{C}[x_1, \ldots, x_n]$, prove that $\{\textsc{Rem}(h_i, G, >)\}_i$ are linearly dependent if and only if there are $\lambda_1, \ldots, \lambda_r \in \mathbb{C}$ such that $\sum_i \lambda_i \, h_i \in I$.*

[1] Computer Algebra Software

$\longrightarrow$ **Hint**: Prove that $\textsc{Rem}(\textsc{Rem}(h_i, G, >) + \textsc{Rem}(h_j, G, >), G, >) = \textsc{Rem}(h_i + h_j, G, >)$. Remember, $\textsc{Rem}(h_i, G, >) = 0 \iff h_i \in I$.

Exercise 5.5 *If G is a Gröbner bases of I such that for each $i \in \{1, \ldots, n\}$, there is $g_i \in G$ such that $\mathrm{LM}_>(g_i)$, then I is zero dimensional.*

$\longrightarrow$ **Hint**: For a fixed i, prove that the sequence $\{\textsc{Rem}(x_i^j, G, >)\}_j$ is linearly dependent. For this, recall that $\textsc{Supp}(\{\textsc{Rem}(x_i^j, G, >)\}_j)$, that is, the monomials appearing in the reminder, can not be divided by the leading monomials of elements in G.

5.2 The shape of zero dimensional systems

In this section, consider G a Gröbner basis of a zero dimensional ideal I with respect to the lexicographical monomial order $>_{\mathrm{LEX}}$. Recall $x_1 >_{\mathrm{LEX}} x_2 >_{\mathrm{LEX}} \cdots >_{\mathrm{LEX}} x_n$.

Exercise 5.6 *Show that there is $h_n(x_n) \in G \cap \mathbb{C}[x_n]$.*

Exercise 5.7 *Assume that I is radical, i.e. $I = \sqrt{I}$, and the last coordinate of each solution is different, that is if $p, \bar{p} \in V_{\mathbb{C}^n}(I)$ are different, then $p_n \neq \bar{p}_n$. Show that, for every x_i, there is a polynomial $h_i(x_n)$ such that $x_i - h_i(x_n) \in I$.*

$\longrightarrow$ **Hint**: Use Lagrange interpolation.

Exercise 5.8 *Prove that, under the previous assumptions, there is a Gröbner basis of I with respect to $>_{\mathrm{LEX}}$ of the following shape:*

$$\left\{ \begin{array}{c} x_1 - h_1(x_n) \\ \vdots \\ x_{n-1} - h_1(x_n) \\ h_n(x_n) \end{array} \right\} \tag{1}$$

$\longrightarrow$ **Hint**: Consider the monomial ideal generated by the polynomials in Equation 1.

Whenever a Gröbner basis looks like Eq. 1, we say that it is in *shape position*. Not every ideal can be written in this way, but radical ones can. The interested reader can find more information in [BMMT94].

The bit-size of this representation might be double exponential in the number of variables. A way of sorting out this problem is to use a Rational Univariate Representation (RUR), where we replace each $h_i(x_n)$ by a rational function. We refer the interested reader to [Rou99].

5.3 Change of ordering - FGLM algorithm

In this exercise you will prove how, in the zero dimensional case, you can transform one Gröbner basis with respect to some monomial order into any other one with respect to other order. This algorithm is called `FGLM` and was introduced in [FGLM93].

Exercise 5.9 *Show that, if G is a Gröbner basis of I with respect to $>$,*

$$\textsc{LinearSpan}_{\mathbb{C}}(\{x^\alpha : (\forall f \in I)\mathrm{LM}_>(f) \nmid x^\alpha\}) = \textsc{LinearSpan}_{\mathbb{C}}(\{\textsc{Rem}(g, G, >) : g \in \mathbb{C}[x_1, \ldots, x_n]\}). \tag{2}$$

Exercise 5.10 *Prove that the vector space from Equation 2 is a finite dimensional vector space if and only if I is zero-dimensional.*

$\longrightarrow$ **Hint**: See Exercise 5.5

Algorithm 2 FGLM

```
Require: Gröbner basis $G$ of zero dimensional ideal $I$ with respect to $>$ and new mon. ordering $\tilde{>}$.
Ensure: Gröbner basis $\tilde{G}$ of $I$ with respect to $\tilde{>}$.
  $L \leftarrow \{\boldsymbol{x}^{\boldsymbol{\gamma}} \in \mathbb{C}[x_1, \dots, x_n]\}$.        # Every monomial in $\mathbb{C}[x_1, \dots, x_n]$
  $B \leftarrow \emptyset$.
  $\tilde{G} \leftarrow \emptyset$.
  while $L \neq \emptyset$ do
    $\boldsymbol{x}^{\boldsymbol{\alpha}} \leftarrow$ minimal element in $L$ with respect to $\tilde{>}$.
    if $\textsc{Rem}(\boldsymbol{x}^{\boldsymbol{\alpha}}, G, >) \in \textsc{LinearSpan}_{\mathbb{C}}(\{\textsc{Rem}(x^\beta, G, >) : x^\beta \in B\})$ then
      Compute $\{\lambda_\beta\}_{x^\beta \in B} \subset \mathbb{C}$ such that $\textsc{Rem}(\boldsymbol{x}^{\boldsymbol{\alpha}}, G, >) + \sum_{x^\beta \in B} \lambda_\beta \, \textsc{Rem}(x^\beta, G, >) = 0$.
      $\tilde{G} \leftarrow \tilde{G} \cup \{\boldsymbol{x}^{\boldsymbol{\alpha}} + \sum_{x^\beta \in B} \lambda_\beta \, x^\beta\}$.
      $L \leftarrow L \setminus \{x^\gamma \in L : \boldsymbol{x}^{\boldsymbol{\alpha}}$ divides $x^\gamma\}$.
    else
      $B \leftarrow B \cup \{\boldsymbol{x}^\alpha\}$.
    end if
  end while
  return $\tilde{G}$.
```

Exercise 5.11 *Prove that if I is zero dimensional, then* FGLM *algorithm terminates and computes a minimal reduced Gröbner basis of I with respect to $\tilde{>}$.*

$\longrightarrow$ **Hint**: Use Exercise 5.4

6 Elimination theory

Given an ideal $I \subset \mathbb{C}[x_1, \dots, x_n]$, we define its i-th elimination ideal $I_i := I \cap \mathbb{C}[x_{i+1}, \dots, x_n]$. We define the i-th projection as the map $\pi_i : \mathbb{C}^n \to \mathbb{C}^{n-i}$, $\pi_i(p_1, \dots, p_n) = (p_{n+1}, \dots, p_n)$.

Exercise 6.1 *Show that given $f, g \in I$, $\texttt{res}(f, g, x_1) \in I_1$.*

Exercise 6.2 (Closure theorem) *Prove that, for each i, $V_{\mathbb{C}^{n-i}}(I_i) = \overline{\pi_i(V_{\mathbb{C}^n}(I))}$.*

$\longrightarrow$ **Hint**: Prove each inclusion independently. Prove that, if $f \in I(\pi_i(V_{\mathbb{C}^n}(I)))$, then $f \in \sqrt{I}$ and it does not involve any of the variables $x_1, \dots, x_i$.

Exercise 6.3 (Extension theorem) *Consider $I := \langle f_1, \dots, f_s \rangle \subset \mathbb{C}[x_1, \dots, x_n]$. We write each f_i as follows,*

$$f_i = c_i(x_2, \dots, x_n) \, x_i^{d_i} + (\textit{terms of degree smaller than } d_1 \textit{ with respect to } x_1),$$

where $c_i \in \mathbb{C}[x_2, \dots, x_n]$ is non-zero. Consider $(p_2, \dots, p_n) \in V_{\mathbb{C}^{n-1}}(I_1) \setminus V_{\mathbb{C}^{n-1}}(c_1, \dots, c_s)$, that is, there is i such that $c_i(p_2, \dots, p_n) \neq 0$. Then, there is $p_1 \in \mathbb{C}$ such that $(p_1, \dots, p_n) \in V_{\mathbb{C}^n}(I)$.

$\longrightarrow$ **Hint**: With no loss of generality, assume that $c_1(p_2, \dots, p_n) \neq 0$. Consider the ideal $J \subset \mathbb{C}[x_1]$ given by partially evaluating every polynomial in I at $(p_2, \dots, p_n)$.

- Prove that there is $\bar{f}_*(x_1)$ be such that $\langle \bar{f}_*(x_1) \rangle = J$.
- Show that every solution $p_1 \in \mathbb{C}$ of $\bar{f}_*(x_1)$ leads to a solution $(p_1, \dots, p_n) \in V(I)$.
- To show that $\bar{f}_*(x_1)$ has solutions, show that $\texttt{GCD}(\bar{f}_*, f_1(x_1, p_2, \dots, p_n)) \neq 1$
  - Show that there is $f_*(x_1, \dots, x_n) \in I$ such that $\bar{f}_*(x_1) = f_*(x_1, p_2, \dots, p_n)$.
  - Prove that the evaluation of $\texttt{res}(f_*, f_1, x)$ at $(p_2, \dots, p_n) \in V(I_1)$ is zero.

– By extending straightforwardly Exercise 1.3, show that $\mathtt{res}(\bar{f}_*, f_1(x_1, p_2, \ldots, p_n), x_1)$ is zero.

Definition 9 *Given a monomial ordering $>$ for $\mathbb{C}[x_1, \ldots, x_n]$, we say that it is an i-elimination order if any monomial $x^\alpha \in \mathbb{C}[x_1, \ldots, x_n]$ involving at least variables in $\{x_1, \ldots, x_i\}$ is bigger with respect to $>$ than any monomial $x^\beta \in \mathbb{C}[x_{i+1}, \ldots, x_n]$.*

Exercise 6.4 *Let $>$ be an i-elimination order. Prove that if G is a Gröbner basis of an ideal $I \subset \mathbb{C}[x_1, \ldots, x_n]$ with respect to $>$, then $G \cap \mathbb{C}[x_{i+1}, \ldots, x_n]$ is a Gröbner basis of the i-th elimination ideal I_i.*

Exercise 6.5 *Present an example of an i-elimination order which is not a lexicographical order.*

6.1 Intersection of ideals

Exercise 6.6 *Prove that the intersection of two ideals is an ideal.*

Exercise 6.7 *Let $R := \mathbb{C}[x_1, \ldots, x_n]$. Given two ideals $I = \langle f_1, \ldots, f_s \rangle, J = \langle \bar{f}_1, \ldots, \bar{f}_r \rangle \subset R$, show that*

$$I \cap J = \langle t\, f_1, \ldots, t\, f_s, (1-t)\, \bar{f}_1, \ldots, (1-t)\, \bar{f}_r \rangle_{R[t]} \cap R.$$

$\longrightarrow$ **Hint**: Note that, for any $h \in R$, $h = t\, h + (1-t)\, h$. Consider evaluating t at 0 and 1.

6.2 Saturation of ideals

Definition 10 *Given two ideals I, J, we define the saturation of I with respect to J as*

$$(I : J^\infty) := \{f \in \mathbb{C}[x_1, \ldots, x_n] : (\forall g \in J)(\exists k \in \mathbb{N}) f\, g^k \in I\}.$$

Exercise 6.8 *Prove that $(I : J^\infty)$ is an ideal.*

Exercise 6.9 *Let $I = \langle f_1, \ldots, f_r \rangle$ be an ideal in $R := \mathbb{C}[x_1, \ldots, x_n]$ and consider $g \in R$. Let t be a new variable. Prove that*

$$I : \langle g \rangle^\infty = \langle f_1, \ldots, f_r, 1 - t\, g \rangle_{R[t]} \cap R.$$

$\longrightarrow$ **Hint**: Extend the argument in the proof of the radical membership algorithm from the second lesson.

Exercise 6.10 *Prove that $g \in \sqrt{I}$ if and only if $1 \in (I : \langle g \rangle^\infty)$.*

Exercise 6.11 *Given three ideals I, J_1, J_2, prove that*

$$(I : (J_1 + J_2)^\infty) = (I : J_1^\infty) \cap (I : J_2^\infty).$$

Exercise 6.12 *Given ideals I, J, prove that $V(I : J^\infty) = \overline{(V(I) \setminus V(J))}$*

$\longrightarrow$ **Hint**: See [CLO15, Thm. 4.4.10].

Recommended bibliography for the course

[1] David A. Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra.* Undergraduate texts in mathematics. Springer, Cham, 4. ed edition, 2015.

[2] Martin Kreuzer and Lorenzo Robbiano. *Computational Commutative Algebra 1.* Springer-Verlag, Berlin Heidelberg, 2000.

[3] Gert-Martin Greuel and Gerhard Pfister. *A Singular Introduction to Commutative Algebra.* Springer, Berlin, Heidelberg, 2002.

[4] Bernd Sturmfels. *Solving systems of polynomial equations.* Published for the Conference Board of the Mathematical Sciences by the American Mathematical Society, Providence, R.I, 2002. Meeting Name: CBMS Conference on Solving Polynomial Equations OCLC: ocm50273026.

[5] David Eisenbud. *Commutative Algebra: with a View Toward Algebraic Geometry.* Graduate Texts in Mathematics. Springer-Verlag, New York, 2004.

[6] Mateusz Michałek and Bernd Sturmfels. *Invitation to nonlinear algebra*, volume 211. American Mathematical Soc., 2021.

References

[BMMT94] Eberhard Becker, Teo Mora, Maria Grazia Marinari, and Carlo Traverso. The shape of the shape lemma. In *Proceedings of the international symposium on Symbolic and algebraic computation*, pages 129–133, 1994.

[CLO05] David A. Cox, John Little, and Donal O'shea. *Using Algebraic Geometry.* Graduate Texts in Mathematics. Springer-Verlag, New York, 2 edition, 2005.

[CLO15] David A. Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra.* Undergraduate texts in mathematics. Springer, Cham, 4. ed edition, 2015.

[DGPS22] Wolfram Decker, Gert-Martin Greuel, Gerhard Pfister, and Hans Schönemann. Singular 4-3-0 — A computer algebra system for polynomial computations. `http://www.singular.uni-kl.de`, 2022.

[EF17] Christian Eder and Jean-Charles Faugère. A survey on signature-based algorithms for computing gröbner bases. *Journal of Symbolic Computation*, 80:719–784, 2017.

[FGLM93] Jean-Charles Faugère, Patrizia Gianni, Daniel Lazard, and Teo Mora. Efficient computation of zero-dimensional gröbner bases by change of ordering. *Journal of Symbolic Computation*, 16(4):329–344, 1993.

[GKZ94] Israel M. Gelfand, Mikhail M. Kapranov, and Andrei V. Zelevinsky. *Discriminants, Resultants, and Multidimensional Determinants.* Birkhäuser Boston, Boston, MA, 1994.

[Jel05] Zbigniew Jelonek. On the effective nullstellensatz. *Inventiones mathematicae*, 162(1):1–17, 2005.

[Kol88] János Kollár. Sharp effective nullstellensatz. *Journal of the American Mathematical Society*, 1(4):963–975, 1988.

[MM82] Ernst W Mayr and Albert R Meyer. The complexity of the word problems for commutative semigroups and polynomial ideals. *Advances in Mathematics*, 46(3):305–329, December 1982.

[Rou99] Fabrice Rouillier. Solving zero-dimensional systems through the rational univariate representation. *Applicable Algebra in Engineering, Communication and Computing*, 9(5):433–461, 1999.

[Stu02] Bernd Sturmfels. *Solving systems of polynomial equations.* Number no. 97 in Conference Board of the Mathematical Sciences regional conference series in mathematics. American Mathematical Soc., Providence, R.I, 2002.