Algebraic Geometry and Algorithms

Elvis Marques
Joana Silva
Martim Costa
João Ruben

24/05/2019

Abstract

Gröbner bases are special sets of polynomials, which are useful to solve problems in many fields, they provide an algorithmic technique that solves a variety of problems. This paper is a very basic introduction to Gröbner Bases and assumes knowledge of linear algebra and introductory ring theory, but should also be of interest to those with prior knowledge of ideals and polynomial rings. The last section contains implementations of algorithms in Sagemath.

1 Introduction

The objective of this paper is to show and exemplify some concepts that are useful for a better comprehension of Gröbner Bases of a finite ideal. There are a lot of problems that motivate the introduction of Gröbner Basis, such that the ideal membership problem in subspaces $\mathbb{K}[x_1, \ldots, x_n]$, i.e., given a polynomial decide if it belongs or not to an ideal of a ring of polynomials. Over the years, new concepts and results have developed in the area of Computer Algebra and computer algebraists made significant contributions to the fields of Mathematics and Computer Science. Among these contributions, an outstanding example is the theory and algorithms for Gröbner bases. Gröbner Bases were first introduced in 1965 in Bruno Buchberger's Ph.D. dissertation on performing algorithmic computations in residue classes of polynomial rings and are named after his advisor Wolfgang Gröbner. Their importance wasn't fully realized for several years and the ideas presented here are applicable to any polynomial ring $\mathbb{K}[x_1, \ldots, x_n]$ where $\mathbb{K}$ is a field, and I is an ideal of the ring $\mathbb{K}[x_1, \ldots, x_n]$. The ring that will be used in examples is $\mathbb{Q}[x, y, z]$, which is the set of all possible polynomials in the indeterminants x, y, and z with rational coefficients.

Section two of this paper mostly reviews the elementary theory of polynomials over a field. Since we're focused on the computational aspect of algebra the main result here

is the proof of the division theorem, which is constructive, providing an algorithm which serves as the foundation for the previously mentioned Buchberger's algorithm and thus much of the computational theory surrounding the topic of Gröbner bases. The third section introduces some concepts from algebraic geometry such as varieties, radical ideals, affine spaces and the Nullstellensatz, the latter of which will be useful in proving the two main results of the section. Finally particular computational applications of the theory are explored in the last section with the aid of SageMath.

2 The Algebra of Polynomials

Polynomials as algebraic entities are sequences with only finitely many non-zero elements called *coefficients*. This formalism is introduced because polynomial functions, in general, are not uniquely determined by their corresponding coefficients. However, the theory developed in this assignment is concerned with infinite fields, a domain in which the familiar conception of a polynomial is sufficient. Nonetheless, for the sake of completion some basic definitions are presented.

Definition 2.1. *A* ***monomial*** *in $x_1, \ldots, x_2$ is a product of the form*

$$x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n},$$

with $\alpha_1, \ldots, \alpha_n \in \mathbb{N}$. The ***total degree*** *of this monomial is defined to be $|\alpha| = \sum_{i=1}^{n} \alpha_i$.*

Notation 2.2. *Let $\alpha = (\alpha_1, \ldots, \alpha_n)$ we represent the aforementioned product as*

$$x^{\alpha} = x_1^{\alpha_1} \cdots x_n^{\alpha_n}.$$

Definition 2.3. *A* ***polynomial*** *f in $x_1, \ldots, x_n$ with coefficients in a field $\mathbb{K}$ is a finite linear combination of monomials with coefficients in $\mathbb{K}$. Written as*

$$f = \sum_{\alpha} a_\alpha x^\alpha,$$

The set of all polynomials in $x_1, \ldots, x_n$ over a field $\mathbb{K}$ will be denoted by $\mathbb{K}[x_1, \ldots, x_n]$. Under intuitively defined operations of addition and multiplication, this structure forms commutative ring.

Example 2.4. *Show some polynomials and how they relate to the this notation*

Definition 2.5. *Let $f = \Sigma_\alpha a_\alpha x^\alpha \in \mathbb{K}[x_1, \ldots, x_n]$.*

- *a_α is called the* ***coefficient*** *of the monomial x^α.*
- *If $a_\alpha \neq 0$, then we call $a_\alpha x^\alpha$ a* ***term*** *of f.*

- *If* $f \neq 0$ *then* $\deg(f) = \max\{|\alpha| : a_\alpha \neq 0\}$
- *If* $f = 0$ *then we define* $\deg(f) = -\infty$

Theorem 2.6. *Let* $f, g \in \mathbb{K}[x_1, x_2, \ldots, x_n]$ *be non-zero polynomials. Then*

1. $\deg(fg) = \deg(f) + \deg(g)$
2. *If* $f + g \neq 0$, *then* $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$

Definition 2.7. *Given a field* $\mathbb{K}$ *and* $n \in \mathbb{N}$, *we define the n-dimensional* ***affine space*** *over* $\mathbb{K}$ *to be the set*

$$\mathbb{K}^n := \{(a_1, \ldots, a_n) : a_1, \ldots, a_n \in \mathbb{K}\}.$$

Given $(a_1, \ldots, a_n) \in \mathbb{K}^n$ and $f \in \mathbb{K}[x_1, \ldots, x_n]$, we can replace every x_i by a_i in the expression of f. Due to the multiplicative and additive closure of a field the resulting expression is an element of $\mathbb{K}$. This defines the **polynomial function** of f.

Example 2.8. *Show example where different polynomials define the same function, mention the issue doesn't arise in infinite fields*

2.1 The Ideal Membership Problem

So far we've defined things quite generally, it's worthwhile considering $\mathbb{K}[x]$ in order to fully appreciate the increase in complexity.

In this section, as a motivation for the introduction of Gröbner bases, we will be discussing the **ideal membership problem**. Given polynomials $p_1, \ldots, p_n, g \in \mathbb{K}[x_1, \ldots, x_n]$ and an ideal $I = (p_1, \ldots, p_n) \subseteq K[x_1, \ldots, x_n]$ how do we determine whether or not $g \in I$? It turns out that for $\mathbb{K}[x]$ the solution is quite simple.

2.1.1 Division

In algebra it is proven that every ideal of $\mathbb{Z}$ is generated by a single integer, i.e., $\mathbb{Z}$ is a principal ideal domain. Usually this fact is proven through the use of the gcd which itself requires the division algorithm. It is then natural to wonder if the argument may be generalized. Note also that the ideal membership problem for ideals of $\mathbb{Z}$ is solved through the use of these properties. Given integers $a_1, \ldots, a_n$ and g, we ascertain $g \in I = (a_1, \ldots, a_n)$ by first computing $\gcd(a_1, \ldots, a_n)$ and checking if it is a divisor of g, if it is not then we conclude that $g \notin I$. In $\mathbb{K}[x]$ the process is identical once the appropriate abstractions are introduced.

Proposition 2.9. *Let* $\mathbb{K}$ *be a field and* $p, g \in \mathbb{K}[x]$ *such that* $g \neq 0$, *then there exists unique polynomials* $p, r \in \mathbb{K}[x]$ *such that*

$$p = g \cdot q + r \text{ with } \deg(r) < \deg(p)$$

See [2] for the proof.

The proof of this theorem gives us a division algorithm for polynomials in $K[x]$.

Example 2.10.

$$\begin{array}{r|l} x^3 - 6x^2 - x + 12 & x - 2 \\ \hline -x^3 + 2x^2 & x^2 - 4x - 9 \\ \hline -4x^2 - x + 12 & \\ 4x^2 - 8x & \\ \hline -9x + 12 & \\ 9x - 18 & \\ \hline -6 & \end{array}$$

Here $p = (x-2)(x^2 - 4x - 9) - 6$, $q = x^2 - 4x - 9$ *and* $r = -6$.

2.1.2 Order

An examination of the division algorithm in $\mathbb{K}[x]$ tells us that the notion of *ordering of terms* in polynomials is essential, because the procedure relies on the ability to identify the leading term. No problems emerge for polynomials of a single indeterminate because the choice is clear, the leading term is simply defined to be the monomial with the largest exponent. But how would we order $f = xyz + yz^3$? We may choose by summing the exponents and decide that $\mathrm{LT}(f) = yz^3$ but we may also wish to prioritize the variable x and instead have $\mathrm{LT}(f) = xyz$.

Definition 2.11. *A* ***monomial ordering*** *on* $\mathbb{K}[x_1, \ldots, x_n]$ *is a relation is a relation* $>$ *on* $\mathbb{Z}^n_{\geq 0}$ *satisfying:*

1. $>$ *is a total ordering on* $\mathbb{Z}^n_{\geq 0}$,
2. *If* $\alpha > \beta$ *and* $\gamma \in \mathbb{Z}^n_{\geq 0}$, *then* $\alpha + \gamma > \beta + \gamma$,
3. *If* $A \subseteq \mathbb{Z}^n_{\geq 0}$ *non-empty, then there exists* $\alpha \in A$ *such that* $\beta > \alpha$ *for every* $\beta \neq \alpha$ *in* A.

Next we define the monomial ordering that'll be most frequently used throughout the assignment.

Definition 2.12 (Lexicographic Order)**.** *Let* $\alpha = (\alpha_1, \ldots, \alpha_n)$ *and* $\beta = (\beta_1, \ldots, \beta_n)$ *both be elements of* $\mathbb{Z}^n_{\geq 0}$. *We say* $\alpha >_{lex} \beta$ *if the leftmost nonzero entry of the vector difference* $\alpha - \beta$ *is positive. We write* $x^\alpha >_{lex} x^\beta$ *if* $\alpha >_{lex} \beta$.

The proof that this is indeed a monomial ordering on $\mathbb{Z}^n_{\geq 0}$ is in [1].

Definition 2.13. *Let $f = \Sigma_\alpha a_\alpha x^\alpha$ be a non-zero polynomial in $\mathbb{K}[x_1, \ldots, x_n]$ and let $>$ be a monomial order.*

- $\text{multideg}(f) = \max(\alpha \in \mathbb{Z}^n_{\geq 0} : a_\alpha \neq 0)$*, taken with respect to the fixed order.*
- $\text{LC}(f) = a_{\text{multideg}(f) \in \mathbb{K}}$.
- $\text{LM}(f) = x^{\text{multideg}(f)}$.
- $\text{LT}(f) = \text{LC}(f) \cdot \text{LT}(f)$.

Lemma 2.14. *Let $f, g \in \mathbb{K}[x_1, \ldots, x_n]$ be non-zero polynomials. Then:*

1. $\text{multideg}(f \cdot g) = \text{multideg}(f) + \text{multideg}(g)$.
2. *If $f + g \neq 0$, then* $\text{multideg}(f + g) \leq \max(\text{multideg}(f), \text{multideg}(g))$.
3. *If* $\text{multideg}(f) \neq \text{multideg}(g)$ *and $f + g \neq 0$, then*

$$\text{multideg}(f + g) = \max(\text{multideg}(f), \text{multideg}(g)).$$

Theorem 2.15 (Division Theorem)**.** *Let $\mathbb{K}$ be a field and $(g_1, g_2, \ldots, g_k)$ an ordered k-tuple of polynomials in $\mathbb{K}[x_1, x_2, \ldots, x_n]$. If we fix a monomial order in $\mathbb{K}[x_1, x_2, \ldots, x_n]$, then for any $p \in \mathbb{K}[x_1, x_2, \ldots, x_n]$ there exist polynomials $q_1, q_2, \ldots, q_k, r \in \mathbb{K}[x_1, x_2, \ldots, x_n]$ such that*

$$p = q_1 g_1 + q_2 g_2 + \cdots + q_k g_k + r,$$

where $r = 0$ or r is linear combination of monomials, with coefficients in $\mathbb{K}$, none of which is divisible by any of $\text{LM}(g_1), \text{LM}(g_2), \ldots, \text{LM}(g_k)$.

Proof. Proving the following algorithm's correctness gives us a constructive proof of the theorem.

Algorithm 1 The Division Algorithm in $\mathbb{K}[x_1, \ldots, x_n]$

```
1:  procedure DivAlgMultipleIndeterminates(f, )
2:  input: f_1, ..., f_s, f ∈ K[x_1, ..., x_n]
3:  output: q_1, ..., q_s, r ∈ K[x_1, ..., x_n]
4:      q_1 ← 0; q_2 ← 0; ...; q_s ← 0; r ← 0
5:      p ← f
6:      while p ≠ 0 do
7:          i ← 1
8:          divisionoccurred ← false
9:          while i ≤ s and divisionoccurred = false do
10:             if LT(f_i) | LT(p) then
11:                 q_i ← q_i + LT(p)/LT(f_i)
12:                 p ← p − (LT(p)/LT(f_i))f_i
13:                 divisionoccurred ← true
14:             else
15:                 i ← i + 1
16:         if divisionoccurred = false then
17:             r ← r + LT(p)
18:             p ← p − LT(p)
19:     return q_1, ..., q_s, r
```

For $g = 0$ the algorithm is trivially correct and consequently so is the theorem. Considering then $g \neq 0$ observe the following. We may split the main **while** into two cases. The one where line 10's **if** condition is met at least once, and the case where it is never met. Restated:

1. **Remainder Step:** This is the case when

$$\forall_{i \in \{1,\ldots,s\}} : \mathrm{LT}(f_i) \nmid \mathrm{LT}(p).$$

2. **Division Step:** Which is the negation of the previous, i.e.,

$$\exists_{i \in \{1,\ldots,s\}} : \mathrm{LT}(f_i) \mid \mathrm{LT}(p).$$

First we begin by showing that the equation

$$f = q_1 f_1 + \ldots + q_s f_s + p + r. \tag{1}$$

Suppose (1) holds at one iteration of the loop, as previously established, either a remainder or division step has occurred. If the former is the case then the values of p and r will have changed, but their sum $p + r$ remains the same since $p + r = p(p - \mathrm{LT}(p)) + (r + \mathrm{LT}(p))$

and hence (1) holds. On the other hand, if a division step has occurred, some $\mathrm{LT}(f_i)$ divides $\mathrm{LT}(p)$. The performed computations imply that $q_i f_i + p = (q_i + \mathrm{LT}(p)/\mathrm{LT}(f_i))f_i + (p - (\mathrm{LT}(p)/\mathrm{LT}(f_i))f_i)$, and thus (1) also holds in this case. Since for the first iteration (1) clearly holds, induction implies it to be true at every iteration.

Observations:

1. The algorithm halts when $p = 0$, so if it does halt then (1) becomes

$$f = q_1 f_1 + \ldots + q_s f_s + r.$$

2. The value of r is only altered by adding to its previous state the leading term of whatever p is in that stage of the computation.

3. The value of r is only altered at all when we are dealing with a Remainder Step, that is when the condition $\mathrm{LT}(f_i) \nmid \mathrm{LT}(p)$ is met, consequently it is of the form

$$r = \sum_{g \in \mathcal{D}} \mathrm{LT}(g) = \sum_{g \in \mathcal{D}} \mathrm{LC}(g) \cdot \mathrm{LM}(g)$$

where $\mathcal{D} = \{f_i : \mathrm{LT}(f_i) \nmid \mathrm{LT}(p)\}$.

It remains only to prove the first observation, does this procedure always halt?

In a Remainder Step we assign p the value $p' = p - \mathrm{LT}(p)$. Having $\mathrm{multideg}(p') \geq \mathrm{multideg}(p)$ would be a contradiction, proving that $\mathrm{multideg}(p')$ is strictly less than $\mathrm{multideg}(p)$. In a Division Step, p is assigned the value

$$p' = p - \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} f_i \neq 0.^1 \tag{2}$$

By lemma 2.14 then

$$\mathrm{multideg}\Big(\frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} f_i\Big) = \frac{\mathrm{multideg}(\mathrm{LT}(p))}{\mathrm{multideg}(\mathrm{LT}(f_i))} \mathrm{multideg}(f_i) = \mathrm{multideg}(\mathrm{LT}(p)).$$

Since the leading terms are the same, $\mathrm{multideg}(p') < \mathrm{multideg}(p)$. In conclusion, $\mathrm{multideg}(p)$ decreases at every iteration of the main loop. Eventually it must reach 0, meaning $p = 0$ and the algorithm halts.

□

[1] When $p' = 0$ then the algorithm terminates.

Example 2.16. *Let* $p = -x^2y^2 + x^2y + y^4 - y$, $g_1 = xy - x$, $g_2 = x^2 - x$ *and* $g_3 = y^2 - y$ *be polynomials in* $\mathbb{K}[x, y, z]$ *and fix* $x >_{lex} y$.

$-x^2y^2 - x^2 + x^2y + y^4 - y$	$xy - x$	$x^2 - x$	$y^2 - y$
$x^2y^2 - x^2y$	$-xy$		$y^2 + y + 1$
$y^4 - y$			
$-y^2 + y^3$			
$y^3 - y$			
$-y^3 + y^2$			
$y^2 - y$			
$-y^2 + y$			
0			

p is divisible by g_1, g_2, g_3 *then,*
$-x^2y^2 - x^2 + x^2y + y^4 - y = (xy - x) * (-xy) + (x^2 - x) * 0 + (y^2 - y) * (y^2 + y + 1)$
therefore, $r(x) = 0$, $q_1 = -xy$, $q_2 = 0$, $q_3 = y^2 + y + 1$

Example 2.17. *ordem lexical* $x > y$
$p = x^2 - y$;
$g_1 = x^2y - x$; $g_2 = xy^2 - x$
Therefore we have,

$x^2 - y$	$x^2y - x$	$xy^2 - x$

p is not divisible by g_1 *and* g_2 *then,*
$x^2 - y = (x^2y - x) * 0 + (xy^2 - x) * 0 + x^2 - y$ *therefore,* $r(x) = x^2 - y$, $q_1 = 0$, $q_2 = 0$

Definition 2.18. *An ideal* $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ *is a* ***monomial ideal*** *if there is a subset* $A \subseteq \mathbb{Z}^n_{\geq 0}$ *(possibly infinite) such that* I *consists of all polynomials which are finite sums of the form* $\sum_{\alpha \in A} h_\alpha x^\alpha$, *where* $h_\alpha \in \mathbb{K}[x_1, \ldots, x_n]$. *In this case, we write* $I = (x^\alpha : \alpha \in A)$.

Lemma 2.19. *Let* $I = (x^\alpha : \alpha \in A)$ *be a monomial ideal. Then a monomial* x^β *is in* I, *if and only if,* $x^\beta \mid x^\alpha$ *for some* $\alpha \in A$.

Definition 2.20. *Let* $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ *be an ideal other than* $\{0\}$, *and fix a monomial ordering. Then:*

1. *We define* $\mathrm{LT}(I) = \{cx^\alpha = \mathrm{LT}(f) : f \in I \setminus \{0\}\}$,

2. *and* $\mathrm{LTId}(I) = (\mathrm{LT}(I))$, *called the* ***leading term ideal****.*

Definition 2.21. *Fix a monomial order on* $\mathbb{K}[x_1, \ldots, x_n]$*. A finite subset* $G = \{g_1, \ldots, g_t\}$ *of the ideal* $\{0\} \neq I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ *is said to be a* ***Gröbner basis*** *if*

$$(\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)) = \mathrm{LTId}(I).$$

Proposition 2.22. *The* $I \subset \mathbb{K}[x_1, \ldots, x_n]$ *be an ideal. Then* $\mathbb{K}[x_1, \ldots, x_n]/I$ *is isomorphic as a* $\mathbb{K}$*-vector space to* $S = \mathrm{span}(\mathrm{x}^\alpha : \mathrm{x}^\alpha \notin \mathrm{LTId(I)})$.

Proof. See Proposition 4 of section 3 in chapter 5 of [1]. □

3 Algebraic Geometry

3.1 Affine Varieties

Definition 3.1. *Let* $\mathbb{K}$ *be a field and* $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$*. We define*

$$V(f_1, \ldots, f_s) := \{(a_1, \ldots, a_n) \in \mathbb{K}^n : f_i(a_1, \ldots, a_n) = 0 \wedge 1 \leq i \leq s\},$$

and say that $V(f_1, \ldots, f_s)$ *is the* ***affine variety*** *defined by* $f_1, \ldots, f_s$*.*

Example 3.2. *content...*

Theorem 3.3 (Hilbert's Nullstellensatz - Strong version)**.** *Let* $\mathbb{K}$ *be an algebraically closed field and* $g, g_1, \ldots, g_s \in \mathbb{K}[x_1, \ldots, x_n]$*. Then* $g \in I(V(g_1, \ldots, g_s))$ *if and only if*

$$g^m \in (g_1, \ldots, g_s)$$

for some integer $m \geq 1$*.*

Proof. See Theorem 2 in section 1 of chapter 4 in [1]. □

Definition 3.4. *An ideal* I *is* ***radical*** *if* $f^m \in I$ *for some integer* $m \geq 1$ *implies that* $f \in I$*.*

Definition 3.5. *Let* $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ *be an ideal. The* ***radical*** *of* I*, denoted* $\sqrt{I}$*, is the set*

$$\{f : f^m \in I \text{ for some integer } m \geq 1\}$$

Definition 3.6. *Let* $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ *be an ideal, and let* $f, g \in \mathbb{K}[x_1, \ldots, x_n]$*. We say* f *and* g *are* ***congruent modulo*** I*, written*

$$f \equiv g \mod I,$$

if $f - g \in I$*.*

Example 3.7. *$I = (x^2 - y^2, x + y^3 + 1) \subseteq \mathbb{K}[x, y]$, then $f = x^4 - y^4 + x$ and $g = x + x^5 + x^4y^3 + x^4$ are congruent modulo I since*

$$\begin{aligned} f - g &= x^4 - y^4 - x^5 - x^4y^3 - x^4 \\ &= (x^2 - y^4)(x^2 - y^2) - (x^4)(x + y^3 + 1) \in I \end{aligned}$$

Importantly the congruence relation forms an equivalence relation on $\mathbb{K}[x_1, \ldots, x_n]$. Hence we can talk about the equivalence class of any $f \in \mathbb{K}[x_1, \ldots, x_n]$, denoted as

$$[f] = \{g \in \mathbb{K}[x_1, \ldots, x_n] : g \equiv f \mod I\}.$$

Definition 3.8. *The **quotient** of $\mathbb{K}[x_1, \ldots, x_n]$ modulo I. written $\mathbb{K}[x_1, \ldots, x_n]/I$, is the set of equivalence classes for congruence modulo I:*

$$\mathbb{K}[x_1, \ldots, x_n]/I = \{[f] : f \in \mathbb{K}[x_1, \ldots, x_n]\}.$$

Example 3.9. *Let $n\mathbb{Z}$ be an ideal of $\mathbb{Z}$. Note that $a, b \in \mathbb{Z} \Rightarrow a-b \in n\mathbb{Z} \Leftrightarrow n \mid a-b \Leftrightarrow a \equiv b \mod n$. Therefore, $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\} = \{0+n\mathbb{Z}, 1+n\mathbb{Z}, \ldots, (n-1)+n\mathbb{Z}\}$.*

Theorem 3.10. *Fix a monomial ordering in $\mathbb{C}[x_1, \ldots, x_n]$ and let I be an ideal of $\mathbb{C}[x_1, \ldots, x_n]$. Then the following statements are equivalent:*

(i) The affine variety $V = \boldsymbol{V}(I)$ is a finite set.

(ii) For each i, $1 \leq i \leq n$, there is some $m_i \geq 0$ such that $x_i^{m_i} \in \mathrm{LTId}(I)$.

(iii) 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 $x_i^{m_i} = \mathrm{LM}(g)$ for some $g \in G$.

(iv) The $\mathbb{C}$-vector space generated by all the monomials $x^{\boldsymbol{\alpha}}$ such that $x^{\boldsymbol{\alpha}} \notin \mathrm{LTId}(I)$ is finite-dimensional.

(v) The $\mathbb{C}$-vector space $\mathbb{C}[x_1, \ldots, x_n]/I$ is finite-dimensional.

Proof. (i) $\Rightarrow$ (ii): If $V = \emptyset$ the Weak Nullstellensatz tells us $I = \mathbb{C}[x_1, \ldots, x_n]$, it follows that $1 \in I$. Fix $m_i = 0$ for every i, then $x_i^0 = 1 \in \mathrm{LTId}(I)$. Assume $\#V = m \in \mathbb{N}$, then we list all m elements $e_1, \ldots, e_m \in V \subset \mathbb{C}^n$ (we can do this since every finite set is countable). For a fixed i we can construct the following one-variable polynomial:

$$f(x_i) = \prod_{j=1}^{m} (x_i - a_j),$$

where a_j is the j-th coordinate of $e_j = (a_1, \ldots, a_n)$. f vanishes at every point of V, so $f \in \mathbf{I}(V)$. By the Nullstellensatz, there is some $N \geq 1$ such that $f^N \in I$. This implies

that $\mathrm{LM}(f^N) \in \mathrm{LTId}(I)$. Repeated application of the distributive property shows that $\mathrm{LM}(f^N) = x_i^{Nm} \in \mathrm{LTId}(I)$.

(ii) $\Leftrightarrow$ (iii) Let $x_i^{m_i} \in \mathrm{LTId}(I)$ and G be a Gröbner basis of I, by definition we have that $\mathrm{LTId}(I) = (\mathrm{LT}(g) : g \in G)$, and thus $x_i^{m_i} \in (\mathrm{LT}(g) : g \in G)$, which is a monomial ideal. By Lemma 2.19, there exists a g such that $\mathrm{LT}(g) \mid x_i^{m_i} \Rightarrow \mathrm{LM}(g) \mid x_i^{m_i}$, hence $\mathrm{LM}(g)$ is a power of x_i (by Lemma 2.14). The opposite implication follows directly from the definition of $\mathrm{LTId}(I)$ since $G \subseteq I$.

(ii) $\Leftrightarrow$ (iv) If $x_i^{m_i} \in \mathrm{LTId}(I)$ for each i, then the monomials $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ for which some $\alpha_i \geq m_i$ are all in $\mathrm{LTId}(I)$. The monomials in the complement of $\mathrm{LTId}(I)$ must have $0 \leq a_i \leq m-1$ for each i. As a result, the number of monomials in the complement of $\mathrm{LTId}(I)$ is at most $m_1 \cdot m_2 \cdots m_n$. For the opposite implication assume that the complement consists of $N < \infty$ monomials. Then, for each i, at least one of the $N+1$ monomials $1, x_i, x_i^2, \ldots, x_i^N$ must lie in $\mathrm{LTId}(I)$.

(iv) $\Leftrightarrow$ (v) Follows directly from Proposition 2.22.

(v) $\Rightarrow$ (i) To show that V is finite, it suffices to show that for each i there can be only finitely many distinct i-th coordinates for the points of V. Fix i and consider the classes $[x_i^j]$ in $\mathbb{C}[x_1, \ldots, x_n]/I$, where $j = 0, 1, 2, \ldots$. Since $\mathbb{C}[x_1, \ldots, x_n]/I$ is finite-dimensional, the $[x_i^j]$ must be linearly dependent in $\mathbb{C}[x_1, \ldots, x_n]/I$. Thus, there exist constants c_j (not all zero) and some m such that

$$\sum_{j=0}^{m} c_j [x_i^j] = \Big[\sum_{j=0}^{m} c_j x_i^j \Big] = [0].$$

However, this implies that $\sum_{j=0}^{m} c_j x_i^j \in I$. Since a nonzero polynomial can have only finitely many roots in $\mathbb{C}$, this shows that the points of V have only finitely many i-th coordinates. $\square$

Theorem 3.11. *Let I be an ideal of $\mathbb{C}[x_1, \ldots, x_n]$ such that $V(I)$ is a finite set. Then*

(i) The number of points in $V(I)$ is at most $\dim(\mathbb{C}[x_1, \ldots, x_n]/I)$.

(ii) If I is a radical ideal, the number of points in $V(I)$ is exactly $\dim(\mathbb{C}[x_1, \ldots, x_n]/I)$.

Proof. We first show that given distinct points $p_1, \ldots, p_n \in \mathbb{C}^n$, there is a polynomial $f_1 \in \mathbb{C}[x_1, \ldots, x_n]$ with $f_1(p_1) = 1$ and $f_1(p_2) = \cdot = f_1(p_m) = 0$. To prove this, note that if $a \neq b \in \mathbb{C}^n$, then they must differ at some coordinate, say the j-th, and it follows that $g = (x_j - b_j)/(a_j - b_j)$ satisfies $g(a) = 1, g(b) = 0$. If we apply this observation to each pair $p_1 \neq p_i$, $i \geq 2$, we get polynomials g_i such that $g_i(p_i) = 1$ and $g_i(p_i) = 0$ for $i \geq 2$. Then $f_1 = g_2 \cdot g_3 \cdots g_m$ in turn, we get polynomials $f_1, \ldots, f_m$ such that $f_i(p_i) = 1$ and $f_i(p_j) = 0$ for $i \neq j$.

Now we can prove the proposition. Suppose that $V = \{p_1, \ldots, p_m\}$, where the p_i are distinct. Then we get $f_1, \ldots, f_m$ as above. If we can prove that $[f_1], \ldots, [f_m] \in$

$\mathbb{C}[x_1, \ldots, x_n]/I$ are linearly independent, then:

$$m \leq \dim(\mathbb{C}[x_1, \ldots, x_n]/I) \tag{3}$$

will follow, and the first part of the proposition will be proved. To prove linear independence, suppose that $\sum_{i=1}^{m} a_i[f_i] = [0]$ in $\mathbb{C}[x_1, \ldots, x_n]/I$, where $a_i \in \mathbb{C}$. Back in $\mathbb{C}[x_1, \ldots, x_n]$, this means that $g = \sum_{i=1}^{m} a_i f_i \in I$, so that g vanishes at all points of $V = \{p_1, \ldots, p_m\}$. Then, for $1 \leq j \leq m$, we have

$$0 = g(p_j) = \sum_{i=1}^{m} a_i f_i(p_j) = 0 + a_j f_j(p_j) = a_j,$$

and linear independence follows.

Finally, suppose that I is radical. To prove that equality holds in 3, it suffices to show that $[f_1], \ldots, [f_m]$ form a basis of $\mathbb{C}[x_1, \ldots, x_n]/I$. Since we just proved linear independence, we only need to show that they span. Thus, let $[g] \in \mathbb{C}[x_1, \ldots, x_n]/I$ be arbitrary, and set $a_i = g(p_i)$. Then consider $h = g - \sum_{i=1}^{m} a_i f_i$. One easily computes $h(p_j) = 0$ for all j, so that $h \in \mathbf{I}(V)$. By the Nullstellensatz, $\mathbf{I}(V) = \mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$ since $\mathbb{C}$ is algebraically closed, and since I is radical, we conclude that $h \in I$. Thus $[h] = [0]$ in $\mathbb{C}[x_1, \ldots, x_n]/I$, which implies $[g] = \sum_{i=1}^{m} a_i[f_i]$. Completing the proof. □

4 Computational Applications

The following are implementations of Buchberger's Algorithm and an algorithm for reducing a Gröbner basis in SageMath. These depend on the functions **spoly** and **multpolydiv** which were provided by professor Jorge Nélio, the only other dependency is the package **itertools** which is included in any standard python distribution.

```
def buchberger(polys, ring):
  G = polys
  while True:
    Gp = G
    for i in itertools.combinations(Gp, 2):
      q, r = multpolydiv(spoly(i[0],i[1], ring), G)
      if r != 0:
        G += [r]
    if G == Gp:
      break
  return G
```

1: Buchberger's Algorithm

```
def reduce_basis(basis):
  reduced_basis = []
```

```
  for poly in basis:
    if poly.lc() == 1:
      reduced_basis += [poly]
    else:
      reduced_basis += [poly.lc()^(-1) * poly]
  return reduced_basis
```

2: Algorithm for reducing a Gröbner Basis

Example 4.1. *Consider the ideal in* $\mathbb{Q}[x, y]$

$$I = (2x^2 - xy + 2y^2 - 2, x^2 - xy + y^2 - 1).$$

In order to compute a Gröbner basis for I*, with lexicographic order* $x > y$*, we will use Buchberger's algorithm. First, we consider the set*

$$\begin{aligned} G &= \{g_1, g_2\} \\ &= \{2x^2 - xy + 2y^2 - 2, x^2 - xy + y^2 - 1\}, \end{aligned}$$

and proceed to calculate $\operatorname{lcm}(\mathrm{LM}(g_1), \mathrm{LM}(g_2)) = \operatorname{lcm}(x^2, x^2) = x^2$*. The next step is to calculate the s-polynomial of* g_1 *and* g_2*.*

$$\begin{aligned} S(g_1, g_2) &= \frac{x^2}{2x^2}(2x^2 - xy + 2y^2 - 2) - \frac{x^2}{x^2}(x^2 - xy + y^2 - 1) \\ &= x^2 - \frac{xy}{2} + y^2 - 1 - x^2 + xy - y^2 + 1 \\ &= \frac{xy}{2}. \end{aligned}$$

Now, using the generalized division algorithm, we perform a division of $\frac{xy}{2}$ *by* (g_1, g_2)*.*

$$\begin{array}{c|c|c} \frac{xy}{2} & 2x^2 - xy + 2y^2 - 2 & x^2 - xy + y^2 - 1 \end{array}$$

The output of the algorithm would then be $q_1 = 0, q_2 = 0$ *and* $r = x^2 - y \neq 0$*, since* $r \neq 0$ *we "add it to* G*" obtaining a new set* $G_1 = G \cup \{r\}$*. Now the process repeats, for* G_1*. We begin by computing the s-poly of* g_1 *and* g_3*.* $\operatorname{lcm}(\mathrm{LM}(g_1), \mathrm{LM}(g_3)) = x^2y$*, thus*

$$\begin{aligned} S(g_1, g_3) &= \frac{x^2y}{2x^2}(2x^2 - xy + 2y^2 - 2) - \frac{x^2y}{\frac{xy}{2}}(\frac{xy}{2}) \\ &= x^2y - \frac{xy^2}{2} + \frac{2y^3}{2} - y - x^2y \\ &= -\frac{xy^2}{2} + y^3 - y. \end{aligned}$$

Division algorithm:

$-\frac{xy^2}{2}+y^3-y$	$2x^2-xy+2y^2-2$	x^2-xy+y^2-1	$\frac{xy}{2}$
$\frac{xy^2}{2}$			$-y$
y^3-y			

So, $r = y^3 - y \neq 0$. *The algorithm now repeats for* $G_2 = G_1 \cup \{y^3 - y\}$. *Skipping intermediate calculations:* $\operatorname{lcm}(\operatorname{LM}(g_1, g_4)) = \operatorname{lcm}(x^2, y^3) = x^2y^3$. $S(g_1, g_4) = x^2y - \frac{xy^4}{2} + y^5 - y^3$. *On dividing* $S(g_1, g_4)$ *by* G_2, *we get a remainder equal to zero. The same happens when we divide* $S(g_2, g_3)$ *by* G_2 *and when we divide* $S(g_2, g_4)$ *by* G_2. *Since* $S(g_1, g_3) = 0 \cdot g_1 + 0 \cdot g_2 + 0 \cdot g_3 + 4$, *all remainders are equal to zero. The algorithm stops and we conclude that* $G_2 = \{2x^2 - xy + 2y^2 - z, x^2 - xy + y^2 - 1, \frac{xy}{2}, y^3 - y\}$ *is a Groöbner basis for* I. *By definition then,* $\operatorname{LTId}(I) = (2x^2, x^2, \frac{xy}{2}, y^3)$. *The exponent vectors of the generators of* $\operatorname{LTId}(I)$ *are:*

$$\alpha(1) = (2, 0), \alpha(2) = (1, 1), \alpha(3) = (0, 3).$$

Hence, the elements of

$$\big((2,0) + \mathbb{Z}^2_{\geq 0}\big) \cup \big((1,1) + \mathbb{Z}^2_{\geq 0}\big) \cup \big((0,3) + \mathbb{Z}^2_{\geq 0}\big)$$

are the exponents vectors of monomials in $\operatorname{LTId}(I)$, *which can be represented by diagrams that we saw in class. As shown in [1] the basis for the vector space* $\mathbb{Q}[x, y]/I$ *is the set of the monomials which are not divisible by the monomials of* $\operatorname{LTId}(I)$. *Thus,* $\{1, x, y, y^2\}$ *is a basis for the vector space* $\mathbb{Q}[x, y]/I$.

Multiplication Table for the elements in the basis: *In order to complete the multiplication table for the basis elements, we need to divide the usual product by the Gröbner basis.*

$\times$	1	x	y	y^2
1	1	x	0	0
x	x	$-y^2+1$	0	0
y	y	0	y^2	y
y^2	y^2	0	y	y^2

Dividing x^2 *by* $(2x^2 - xy + 2y^2 - 2, x^2 - xy + y^2 - 1, \frac{xy}{2}, y^3 - y)$ *gives a remainder equal to* $-y^2 + 1$ *which is a linear combination of the elements of the basis.*

Example 4.2. *If* $(p_1, \ldots, p_n) \subseteq \mathbb{K}[x_1, \ldots, x_n]$ *an ideal, then* $\boldsymbol{V}(I) = \boldsymbol{V}(p_1, \ldots, p_n)$. *Let* $I = (x^2 - xz + y^2, y^2 + z^2 - 1, x^2 - z^2 + 1)$, *its reduced Gröbner basis with lex ordering* $x > y > z$ *is*

$$G = \{x^2 - xz + y^2, y^2 - z^2 - 1, x^2 - z^2 + 1, -xz, -z^3 - z\}.$$

Thus solving the system:

$$\begin{aligned} x^2 - xz + y^2 &= 0 \\ y^2 - z^2 - 1 &= 0 \\ x^2 - z^2 + 1 &= 0 \\ -xz &= 0 \\ -z^3 - z &= 0 \end{aligned}$$

is an equivalent problem to the initially stated. In $\mathbb{Q}^3$*, the solutions are* $(0,0,1),(0,0,-1)$*. In* $\mathbb{C}^3$*, the solutions are* $(0,0,1),(0,0,-1),(i,1,0),(-i,-1,0)$*. The number of solutions in* $\mathbb{Q}^n$ *will always be less than or equal to the number of solutions in* $\mathbb{C}^n$ *since any solution in* $\mathbb{Q}^n$ *is also a solution in* $\mathbb{C}^n$*.*
To compute the dimension of $\mathbb{C}[x,y,z]/I$ *we look at its* LTId *which is equal to* $(x^2, y^2, -xz, z^3)$*, then a basis for the vector space is* $\{1,x,y,z,z^2\} \Rightarrow \dim(\mathbb{C}[x,y,z]/I) = 5$*. Note that both in* $\mathbb{C}^3$ *and* $\mathbb{Q}^3$ *the number of solutions is strictly less than* $\dim(\mathbb{C}[x,y,z]/I) = 5$*.*

Example 4.3. *Let's consider* $V(I) = V(2x^2 - xy + 2y^2 - 2, x^2 - xy + y^2 - 1)$ *and observe the following sage math program:*

```
sage: R.<x,y> = QQ[]
sage: J=R.ideal(2*x^2-x*y+2*y^2-2,x^2-x*y+y^2-1)
sage: J
Ideal (2*x^2 - x*y + 2*y^2 - 2, x^2 - x*y + y^2 - 1) $ of Multivariate
Polynomial Ring in x, y over Rational Field
sage: J.dimension()
0
sage: J.variety()
[{y: 0, x: 1}, {y: 0, x: -1}, {y: 1, x: 0}, {y: -1, x: 0}]
```

With this we can verify that $V(I)$ *is a non-empty subset of* $\mathbb{Q}^2$*. Now, in* $\mathbb{C}^2$ *we have:*

```
sage: R.<x,y> = QQ[]
sage: J=R.ideal(2*x^2-x*y+2*y^2-2,x^2-x*y+y^2-1)
sage: J
Ideal (2.0*x^2 - x*y + 2.0*y^2 - 2.0, x^2 - x*y + y^2 - 1.0) of Multivariate
Polynomial Ring in x, y over Complex Field with 53 bits of precision
Field
sage: J.dimension()
0
sage: J.variety()
[{y: 0.0, x: -1.0}, {y: 0.0, x: 1.0}, {y: 1.0, x: 0.0}, {y: -1.0, x: 0.0}]
```

Whit this we can conclude that $V(I)$ hate at most 4 elements in $\mathbb{C}^2$ such as in $\mathbb{Q}^2$, as we have seen before.

References

[1] Cox, D., Little, J. & O'Shea, D., *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, 3rd Edition, Springer-Verlag, 2006.

[2] Ferreira, Jorge N.M., *Lecture Notes for Computational Algebra*, Universidade da Madeira, 2019