PSFPN - Gröbner bases in two variables

Supervisor : Jeremy Berthomieu
Auguste WARME-JANVILLE, Alan PULVAL-DADY

Introduction

Given $f_1 = 0, \ldots, f_r = 0$ where $f_1, \ldots, f_r$ are polynomials in x and y with coefficients in a field $\mathbb{K}$, we are interested in computing solutions of the systems. A Gröbner basis of the ideal $\langle f_1, \ldots, f_r \rangle$ is a set of generators with advantageous properties for solving the system mentioned above and also to guess the belonging or not of a polynomial to the ideal. Studying the structures of these bases is, therefore, a valuable approach for efficiently solving such systems.

It is known that when the system has a finite number of solutions, the associated Gröbner basis under the lexicographical order contains at least two non-zero polynomials that can be distinguished : (1) one exclusively in terms of y and (2) another where the leading term is a power of x. The objective of this project is to investigate the structure of these bases.

To accomplish this, we first examined the construction of a Gröbner basis and then established the existence of polynomials (1) and (2). Subsequently, we explored the structure of the intersection of two Gröbner bases with specific properties (Section 5).

Finally, we extended our analysis to the structure of the intersection of N Gröbner bases.

We would like to extend our sincere appreciation to our supervisor Jeremy Berthomieu from the LIP6 PolSys team for his invaluable guidance and expertise throughout this project.

1 Ideals

Definition 1.1 (Ideal)**.** *Let $(R, +, \cdot)$ be a ring. I is an ideal of R if :*

- *I is a subgroup of $(R, +)$*
- *For all $x \in R$ and $i \in I$, $x \cdot i \in I$*

We will assume that all the rings we work on are commutative.

Definition 1.2 (Principal Ideal)**.** *An ideal I of a ring R is called principal if it is generated by a single element f of R, i.e.*

$$I = \{f \cdot a \mid \forall a \in R\}$$

Such an ideal will be denoted $\langle f \rangle$.

We will also define the intersection and the sum of two ideals, as they will be used later on.

Definition 1.3. *Let $I_1 = \langle f_1, \dots, f_r \rangle$ and $I_2 = \langle g_1, \dots, g_s \rangle$ two ideals of R.*

$$I_1 + I_2 = \{f + g \mid f \in I_1, g \in I_2\}$$

Definition 1.4. *Let I_1, I_2 two ideals of R.*

$$I_1 \cdot I_2 = \{\sum_i f_1 f_2 \mid f_1 \in I_1, f_2 \in I_2\}$$

Proposition 1.1. *Let I_1, I_2 two ideals of R.*

$$I_1 \cdot I_2 \subseteq I_1 \cap I_2$$

Proof. Let $f \in I_1 \cdot I_2$. By definition, $f \in I_1$ as the operator $(\cdot)$ is absorbant. Same goes for I_2, hence the result. □

2 Monomial orderings

When studying polynomials of only one variable, the order of the monomials is straightforward : we implicitly assume that $1 < x < x^2 < \dots$. If we rise the number of variables we study, we can still sort all the powers of one variable with each other, but how do we manage monomials that are products of more than one variable ? There are many ways to handle this order problem. This is why we'll introduce *monomial orderings*.

Definition 2.1 (Monomial ordering)**.** *A monomial ordering $\prec$ on $\mathbb{K}[x, y]$ is any ordering on the monomials $x^i y^j$:*

- *$\prec$ is a total order*
- *If $w \neq 1$ is a monomial of $\mathbb{K}[x, y]$ then $1 \prec w$*
- *If w is a monomial of $\mathbb{K}[x, y]$ and if $u \prec v$ then $uw \prec vw$*

Definition 2.2 (Lexicographic order)**.** *The lexicographic order $\prec_{lex}$ is the monomial order over $\mathbb{K}[x, y]$ defined as :*

$$\forall i \in \mathbb{N}, y^i \prec_{lex} x$$

Proposition 2.1. *For all $i, j, k, l \in \mathbb{N}$, $x^i y^j \prec_{lex} x^k y^l$ if and only if one of the following conditions are satisfied :*

- *$i < k$*
- *$i = k$ and $j < l$*

Proof. $\Rightarrow$
$y^m \prec_{lex} x^m$ 2.2, $y^{m+l} \prec_{lex} y^l x^m$ 2.1, $x^i y^{m+l} \prec_{lex} y^l x^{m+i}$ 2.2, if we let $j = m + l$ and $k = m + i$ we get that $m + i > i \Rightarrow k > i$
$\Leftarrow$ Suppose that we have $i < k$. We can then write
$x^i \prec_{lex} x^k$ 2.2, $x^i y^j \prec_{lex}, x^k y^j$ 2.1, $x^k y^j \prec_{lex} x^{k+1} y^j$ 2.2, 2.1, $x^k y^j y^w \prec_{lex} x^{k+1} y^j y^w$ 2.1, $x^i y^j \prec_{lex} x^k y^j \prec_{lex} x^{k'} y^l$ 2.1, $x^i y^j \prec_{lex} x^{k'} y^l$

□

Definition 2.3 (DRL order)**.** *The DRL (Degree Reverse Lexicographic) order $\prec_{drl}$ is a monomial order over $\mathbb{K}[x, y]$ defined as :*

- $y \prec_{drl} x$
- *For all $i, j, k, l \in \mathbb{N}$, $x^i y^j \prec_{drl} x^k y^l$ if and only if one of the following conditions are satisfied :*
  - $i + j < k + l$.
  - $i + j = k + l$ *and* $j > l$.

Example 2.1. *The first monomials for the DRL order appearing in $\mathbb{K}[x, y]$ are :*
$1 \prec_{drl} y \prec_{drl} x \prec_{drl} y^2 \prec_{drl} xy \prec_{drl} x^2 \prec_{drl} y^3 \prec_{drl} xy^2 \prec_{drl} x^2 y \prec_{drl} x^3 \prec_{drl} \dots$

Definition 2.4. *Let $f \in \mathbb{K}[x, y]$ be a nonzero polynomial and $\prec$ a monomial order.*

- *$LM_\prec(f)$ is the leading monomial of f for $\prec$.*
- *$LC_\prec(f)$ is the leading coefficient of f for $\prec$.*
- *$LT_\prec(f) = LM_\prec(f) \cdot LC_\prec(f)$ is the leading term of f for $\prec$.*

Lemma 2.1. *Let f and g be two polynomials of $\mathbb{K}[x, y]$, and $\prec$ a monomial ordering. Then,*

$$LM_\prec(f \cdot g) = LM_\prec(f) \cdot LM_\prec(g)$$

Proof. Let us first rewrite the polynomials F and G. We have $f = LM(f) + f'$ and $g = LM(g) + g'$, with f', g' in $\mathbb{K}[x, y]$. By definition, we have $LM_\prec(g') \prec LM_\prec(g)$ and $LM_\prec(f') \prec LM_\prec(f)$. Then, by multiplying f and g, we get :

$$f \cdot g = LM(f)LM(g) + LM(f)g' + LM(g)f' + f'g'$$

Since $LM_\prec(g') \prec LM_\prec(g)$ and $LM_\prec(f') \prec LM_\prec(f)$, we get that $LM_\prec(f \cdot g) = LM_\prec(f) \cdot LM_\prec(g)$ □

3 Gröbner Bases

In the section, we will denote I an ideal of the ring $\mathbb{K}[x, y]$.

Definition 3.1 (Gröbner basis)**.** *A finite subset $\mathscr{G} \subseteq I$ is said to be a Gröbner basis of I for the monomial order $\prec$ if for all $f \in I$, there exists $g \in \mathscr{G}$ such that $LM_\prec(g)$ divides $LM_\prec(f)$.*

Definition 3.2 (Staircase)**.** *The staircase $E(I)$ for the monomial order $\prec$ is the set of all the monomials that are not leading monomials of I for $\prec$. It can be expressed as follows :*

$$E(I) = \{x^i y^j \mid \forall (i, j) \in \mathbb{N}^2, \nexists f \in I, LM(f) = x^i y^j\}$$

Proposition 3.1. *Let $\mathscr{G} \subseteq I$ be a Gröbner basis of I for the monomial order $\prec$. Let $m \in \mathbb{K}[x, y]$ be a monomial. $m \in E(I)$ if for all $g \in \mathscr{G}$, $LM_\prec(g)$ does not divide m.*

Proof. Assume that there exists $g \in \mathscr{G}$ such that $LM_\prec(g)$ divides m. Then, there exists a monomial $k \in \mathbb{K}[x, y]$ such that $m = k \cdot LM_\prec(g)$. If we consider the polynomial $f = g \cdot \dfrac{m}{LM(g)}$, we see that we can construct a polynomial of I with m as its leading monomial. So $m \notin E(I)$, hence the result by contraposition. □

Lemma 3.1. *The staircase of I is finite if and only if there exists $k, l \in \mathbb{N}$ such that :*

- *x^k is a leading monomial of I*

- y^l *is a leading monomial of* I

Proof. $\Rightarrow$ Assume the staircase of I is finite. Suppose there exists no $k, l \in \mathbb{N}$ such that either x^k or y^l is a leading monomial of I. Without loss of generality, assume none of the x^k are leading monomials of I. Let $\mathscr{G}$ be a Gröbner basis of I. Then all the leading monomials of $\mathscr{G}$ are either of the form $x^m y^n$, $m, n > 0$ or y^l, $l > 0$. So for all $k > 0$, the monomials x^k are in $E(I)$. Hence $E(I)$ is not finite.
$\Leftarrow$ Conversly, assume there exists $k, l \in \mathbb{N}$ such that x^k and y^l are leading monomials of I. Then, for all $i, j > 0$, $x^k y^i$ and $x^j y^l$ are leading monomials of I (Lemma 2.1), so the the size of $E(I)$ is at most equal to kl. Thus the staircase of I is finite. □

Proposition 3.2. *The staircase of I for a monomial order $\prec$ is a basis of $\mathbb{K}[x, y]/I$ as a $\mathbb{K}$ vector space.*

Proof. All the monomials of $E(I)$ are monomials of the form $x^i y^j$, with all the (i, j) different pairwise. So the monomials of $E(I)$ are linearly independent. $\mathbb{K}[x, y]/I$ is the quotient ring where for all $f \in \mathbb{K}[x, y]/I$, $\nexists m \in LM(I)$ such that m divides $LM(f)$. Thus, by Proposition 3.1, $E(I)$ generates $\mathbb{K}[x, y]/I$. □

Proposition 3.3. *If the staircase of I is finite for a monomial ordering, then it is finite for any monomial ordering.*

Proof. Assume the staircase of I is finite for a monomial order $\prec_1$, it is then a basis of $\mathbb{K}[x, y]/I$. Therefore, we get that any basis of $\mathbb{K}[x, y]/I$ is finite, by definition. So for any monomial ordering $\prec_2$, the staircase of I is finite. □

Theorem 3.1. *If the staircase for the monomial ordering $\prec_1$ is finite, then the staircase for the monomial ordering $\prec_2$ is also finite and has the same cardinal.*

Proof. Let $\prec_1$ a monomial order such that $E_{\prec_1}(I)$ is finite. As proven in Proposition 3.3, $E_{\prec_2}(I)$ is finite. Let us show that $\#E_{\prec_1}(I) = \#E_{\prec_2}(I)$, *i.e.* $dim(E_{\prec_1}(I)) = dim(E_{\prec_2}(I))$. From the dimension theorem for vector spaces, we deduce that $dim(E_{\prec_1}(I)) = dim(E_{\prec_2}(I))$, hence the result. □

Theorem 3.2. *If the staircase of I for the lexicographic order is finite, there exists a non zero polynomial with monomials in y only in I.*

Proof. Let us assume the staircase of I for $\prec_{lex}$ if finite. Then, there exists $l \in \mathbb{N}$ such that y^l is a leading monomial of I. Let $f \in I$ be a polynomial with $LM(f) = y^l$. We can rewrite f as $f = \alpha y^l + f'$. As for all $k \in \mathbb{N}, y^k \prec_{lex} x$ and $LM(f) = y^l$, all the monomials of f' must contain only y as a variable. Thus, $f \in I$ is purely in y. □

Proposition 3.4. *If I is principal and $I \neq \langle 1 \rangle$, the staircase of I is not finite.*

Proof. Let f be the generator of I. Suppose $E(I)$ is finite. So there exists $k, l \in \mathbb{N}$ such that x^k and y^l are leading monomials of I. Then, there exists $i, j \in \mathbb{N}$ such that $i \leq k, j \leq l$ and $x^k = LM_\prec(f) \cdot x^{k-i}$ and $y^l = LM_\prec(f) \cdot y^{l-j}$. So $LM_\prec(f)$ would have to be either only in x or in y, which is not possible as it is unique : contradiction. Thus, $E(I)$ is not finite. □

4 Division over $\mathbb{K}[x, y]$

Using the notion of monimial order, we have a way to sort all the monomials of $\mathbb{K}[x, y]$. Therefore, we can now define a division algorithm similar to the Euclidean division algorithm, which will be useful to prove some results about ideals.

Algorithm 1 Division algorithm over $\mathbb{K}[x, y]$

Input : A polynomial $f \in \mathbb{K}[x, y]$, $\mathscr{G} \subseteq I$
Output : Normal form of f

$h \leftarrow 0$
while $f \neq 0$ **do**
  if there exists g $\in \mathscr{G}$ such that $LM_{\prec}(g)$ divides $LM_{\prec}(f)$ **then**
    $f \leftarrow f - \dfrac{LT_{\prec}(f)}{LT_{\prec}(g)} g$
  else
    $h \leftarrow h + LT_{\prec}(f)$
    $f \leftarrow f - LT_{\prec}(f)$
  end if
end while
return h

Definition 4.1. *Let h be the output of Algorithm 1. If $\mathscr{G}$ is a Gröbner basis of I for the order $\prec$, h is called the normal form of f with respect to $\mathscr{G}$ and $\prec$. In a more formal way,*

$$h = NF(f, \mathscr{G}, \prec)$$

Proposition 4.1. *Let h be the output of Algorithm 1. Every monomial of h is in the staircase of I.*

Proof. In the beginning, $h = 0$. Then, if $\nexists g \in \mathscr{G}$ such that $LM_{\prec}(g)$ divides $LM_{\prec}(f)$, $h \leftarrow LT_{\prec}(f)$. Therefore, every monomial of h is in the staircase of I, as proved above (Proposition 3.1). □

Theorem 4.1. *Let h be the output of Algorithm 1. If $\mathscr{G}$ is a Gröbner basis of I for the order $\prec$, $h = 0$ if and only if $f \in I$.*

Proof. Let $\mathscr{G} = \{g_1, \ldots, g_k\}$ be a Gröbner basis of I.
$\Rightarrow$ Assume that $h = 0$. Using Algorithm 1 on f, we get that :

$$f = \left(\sum_{i=1}^{n} k_i g_i \right)$$

Therefore f is an algebraic combination of elements of $\mathscr{G} \subseteq I$, so $f \in I$.
$\Leftarrow$ Conversly, assume that $f \in I$. Using Algorithm 1 on f, we can write it as :

$$f = \left(\sum_{i=1}^{n} k_i g_i \right) + h$$

Suppose $h \neq 0$, we have :

$$h = f - \left(\sum_{i=1}^{n} k_i g_i \right) \in I.$$

Yet, every monomial of h is in $E(I)$ (Proposition 4.1), so $h \notin I$. We have a contradition, so we deduce that $h = 0$, hence the result. □

Corollary 4.1.1. *Let $\mathscr{G} \subseteq I$ be a Gröbner basis of I for the monomial order $\prec$. Then, $\mathscr{G}$ generates I.*

Proof. Let $f \in I$. If we apply Algorithm 1 to f, we get that

$$f = \sum_{i=1}^{n} k_i g_i + NF(f, \mathscr{G}, \prec)$$

As $NF(f, \mathscr{G}, \prec) = 0$, f is an algebraic combination of elements of $\mathscr{G}$, therefore $\mathscr{G}$ generates I. □

Corollary 4.1.2. *Let h be the output of Algorithm 1. h does not depend on the choices made during the execution of the algorithm.*

Proof. We'll prove that h is unique. Let $f \in \mathbb{K}[x,y]$. Using the Algorithm 1 on f, we get that $f = g + h$ where :

$$g = \sum_{i=1}^{n} k_i g_i$$

Suppose that we have $f = g + h = g' + h'$, where g' is also a combination of elements of $\mathscr{G}$. Then, $h - h' = g' - g \in I$. If $h \neq h'$, there exist $g \in \mathscr{G}$ such that $LT(g)$ divides $LT(h - h')$. But from Proposition 4.1, all the monomials of h and h' are in $E(I)$. In particular, $LT(h - h') \in E(I)$. We get to a contradition, thus $h - h' = 0$ which proves the uniqueness of h. □

5 Geometric point of view

After studying ideals from an algebraic point of view, we may need to observe what happens when we study the zeroes of the polynomials characterizing ideals. Here, we'll introduce affine varieties, and some results linking the algebraic and geometric points of view.

Varieties

Definition 5.1 (Affine variety)**.** *The variety of an ideal I is the set as defined below :*

$$V(I) = \{(a,b) \in \overline{\mathbb{K}} \mid \forall f \in I, f(a,b) = 0\}$$

Where $\overline{\mathbb{K}}$ stands for the algebraic closure of $\mathbb{K}$.

Proposition 5.1. *Let I_1, I_2 two ideals of $\mathbb{K}[x,y]$ such that $I_1 \subseteq I_2$. Then, $V(I_2) \subseteq V(I_1)$.*

Proof. Let $p \in V(I_2)$. Then for all $f_2 \in I_2$, $f_2(p) = 0$. In particular, as $I_1 \subseteq I_2$, for all $f_1 \in I_1$, $f_1(p) = 0$, so $p \in V(I_1)$, hence $V(I_2) \subseteq V(I_1)$. □

Proposition 5.2. *Let I_1, I_2 two ideals of $\mathbb{K}[x,y]$.*

$$V(I_1 \cdot I_2) = V(I_1 \cap I_2)$$

Proof. One can observe that $(I_1 \cap I_2) \cdot (I_1 \cap I_2) \subseteq I_1 \cdot I_2$. Since $I_1 \cdot I_2 \subseteq I_1 \cap I_2$. We then have :

$$(I_1 \cap I_2) \cdot (I_1 \cap I_2) \subseteq I_1 \cdot I_2 \subseteq I_1 \cap I_2$$

Thus,

$$V(I_1 \cap I_2) \subseteq V(I_1 \cdot I_2) \subseteq V((I_1 \cap I_2) \cdot (I_1 \cap I_2))$$

Since $V((I_1 \cap I_2) \cdot (I_1 \cap I_2)) = V(I_1 \cap I_2)$, we can conclude that $V(I_1 \cdot I_2) = V(I_1 \cap I_2)$. □

Proposition 5.3. *Let I_1, I_2 two ideals of $\mathbb{K}[x,y]$.*

(i) $V(I_1 \cdot I_2) = V(I_1) \cup V(I_2)$

(ii) $V(I_1 \cap I_2) = V(I_1) \cup V(I_2)$

(iii) $V(I_1 + I_2) = V(I_1) \cap V(I_2)$

Proof. Let us first write the formal definitions of $V(I_1)$ and $V(I_2)$. We have :

$$V(I_1) = \{(a,b) \in \overline{\mathbb{K}} \mid \forall f_1 \in I_1, f_1(a,b) = 0\},\ V(I_2) = \{(c,d) \in \overline{\mathbb{K}} \mid \forall f_2 \in I_2, f_2(a,b) = 0\}$$

(i)

$$\begin{aligned}
V(I_1 \cdot I_2) &= \{(a,b) \in \overline{\mathbb{K}} \mid \forall f \in I_1 \cdot I_2, f(a,b) = 0\} \\
&= \{(a,b) \in \overline{\mathbb{K}} \mid \forall f_1 \in I_1, \forall f_2 \in I_2, f_1 f_2(a,b) = 0\} \\
&= \{(a,b) \in \overline{\mathbb{K}} \mid \forall f_1 \in I_1, \forall f_2 \in I_2, f_1(a,b) = 0 \vee f_2(a,b) = 0\} \\
&= \{(a,b) \in \overline{\mathbb{K}} \mid \forall f_1 \in I_1, f_1(a,b) = 0\} \cup \{(c,d) \in \overline{\mathbb{K}} \mid \forall f_2 \in I_2, f_2(a,b) = 0\} \\
&= V(I_1) \cup V(I_2)
\end{aligned}$$

(ii) We have that $V(I_1 \cdot I_2) = V(I_1 \cap I_2)$, hence the result.

(iii)

$$\begin{aligned} V(I_1 + I_2) &= \{(a,b) \in \overline{\mathbb{K}} \mid \forall f \in I_1 + I_2, f(a,b) = 0\} \\ &= \{(a,b) \in \overline{\mathbb{K}} \mid \forall f_1 \in I_1, \forall f_2 \in I_2, f_1(a,b) = 0 \wedge f_2(a,b) = 0\} \\ &= V(I_1) \cap V(I_2) \end{aligned}$$

□

Remark 5.1. *We see that as we reduce the generating conditions of the members of the ideal we study, the size of the associated variety rises (while making an intersection of ideals, we get union of varieties). On the other hand, while rising the conditions to belong to an ideal, the size of the associated variety reduces.*

We now want to study the Gröbner basis for the lexicographic ordering (lex-GB) of the intersection of ideals, assuming we their lex-GB. We will start with the simplest case, called the "shape position", which is $I = \langle h(y), x - g(y) \rangle$. Here starts the real *"research"* part of this project.

Ideals Intersections case 1

We will now study ideals based on generators of a certain form. First, let us define the points $p_i = (x_i, y_i)$ for $0 \leq i \leq d$, where $y_i \neq y_j, \forall i, j$. Then, we will define the following polynomials :

$$h(y) = \prod_{i=0}^{d-1} (y - y_i)$$

And the polynomial $g(y) = x$ that can be defined by interpolating the points p_i as all the y_i are distinct. We can now define the following ideal :

$$I = \langle h(y), x - g(y) \rangle$$

Proposition 5.4. *I is a Gröbner basis of I for the lexicographic ordering $\prec_{lex}$.*

Proof. Let $a \in I$. If a is purely in y, then a is a multiple of $h(y)$ and then $LM(h(y))$ divides $LM(a)$. Otherwise, $LM(a) = x^k$ where $k \geq 1$, so $LM(x - g(y)) = x$ divides $LM(a)$. □

Let us now define the ideals I_1 and I_2.

$$I_1 = \langle h_1(y), x - g_1(y) \rangle$$

$$I_2 = \langle h_2(y), x - g_2(y) \rangle$$

We will assume that $\gcd(h_1, h_2) = 1$.

Theorem 5.1. *Let I_1 and I_2 be two ideals as defined above, with g_1 defined by interpolating the points $p_{0,\ldots,d-1}$ and g_2 defined by interpolating the points $p_{d,\ldots,e-1}$*

$$I_1 \cap I_2 = \langle h_1 h_2(y), x - g_3(y) \rangle$$

Where $g_3(y)$ is the polynomial defined by interpolating the points $p_{0,\ldots,d-1,d,\ldots,e-1}$ and satisfies :

$$\begin{cases} g_3 = g_1 \pmod{h_1} \\ g_3 = g_2 \pmod{h_2} \end{cases}$$

Proof. Let us denote $I = \langle h_1 h_2(y), x - g_3(y) \rangle$. One can remark that I is a Gröbner basis of I for $\prec_{lex}$. Also, remark that as $\gcd(h_1, h_2) = 1$, there exists u, v such that :

$$uh_1 + vh_2 = 1$$

We will first show that $I_1 \cap I_2 \subseteq \langle h_1 h_2(y), x - g_3(y) \rangle$. Assume that $f \in I_1 \cap I_2$. We can write f as :

$$f = \sum_{i=1}^{n} m_i$$

Where all the m_i are in $I_1 \cap I_2$.
Let m be any of the m_i. There a few possible cases for m :

- m is purely in y. Then $h_1 | m$ and $h_2 | m$, so $h_1 h_2 | m$, thus $m \in \langle h_1 h_2(y) \rangle$.
- m is a multiple of $x - g_1(y)$ and $x - g_2(y)$. That is, $m = k \cdot h$, h being the polynomial that vanishes on all the $p_{0,\dots,d-1,d,\dots,e-1}$. As all the y_i are distinct, We have that $x - g_3(y) = h$, so $m \in \langle x - g_3(y) \rangle$.
- m is a multiple of h_1 and $x - g_2(y)$. If we divide m by $x - g_3$, we get :

  $$q = h_1, r = h_1(g_2 - g_3)$$

  We can remark that

  $$\begin{aligned} r &= 0 && \pmod{h_1} \\ r &= h_1(g_2 - g_2) && \pmod{h_2} \\ r &= 0 && \pmod{h_2} \end{aligned}$$

  Thus by the CRT, $r = 0 \pmod{h_1 h_2}$, so by Theorem 4.1, $m \in I$
- This point is the same as the last one, we only need to swap h_1 with h_2 and $x - g_2(y)$ with $x - g_1(y)$.

Now, let us show that $\langle h_1 h_2(y), x - g_3(y) \rangle \subseteq I_1 \cap I_2$.

- It is straightforward that $\langle h_1 h_2(y) \rangle \subseteq I_1 \cap I_2$, as it belongs to I_1 as well as I_2.
- Now, we will show that $\langle x - g_3(y) \rangle \subseteq I_1 \cap I_2$. Recall that we have $uh_1 + vh_2 = 1$. Using the CRT, we have :

  $$\begin{aligned} (x - g_2)uh_1 + (x - g_1)vh_2 &= x(uh_1 + vh_2) - ug_2h_1 - vg_1h_2 \\ &= x - g_3(y) \end{aligned}$$

  Thus we get that $\langle x - g_3(y) \rangle \subset I_1 \cap I_2$ as it is an algebraic expression of terms belonging to $I_1 \cap I_2$.

□

Now, assume $\gcd(h_1, h_2) \neq 1$.
We can now write the two ideals as :

$$\begin{aligned} I_1 &= \langle h_1(y), x - g_1(y) \rangle = \langle \alpha p_1(y), x - g_1(y) \rangle \\ I_2 &= \langle h_2(y), x - g_2(y) \rangle = \langle \alpha p_2(y), x - g_2(y) \rangle \end{aligned}$$

Where $\alpha = \gcd(h_1, h_2)$ and $\gcd(p_1, p_2) = 1$.
We will define then define polynomials $g_3(y)$

$$\begin{cases} g_3 = g_1 & \pmod{p_1} \\ g_3 = g_2 & \pmod{p_2} \end{cases}$$

and $f(x, y)$

$$\begin{cases} f = x - g_3 & \pmod{p_1 p_2} \\ f = (x - g_1)(x - g_2) & \pmod{\alpha} \end{cases}$$

Theorem 5.2. *Assume* $\gcd(h_1, h_2) \neq 1$.

$$I_1 \cap I_2 = \langle \operatorname{lcm}(h_1, h_2)(y), \alpha(x - g_3(y)), f(x, y) \rangle$$

Proof. Let us denote $I = \langle \text{lcm}(h_1, h_2)(y), \gcd(h_1, h_2)(x - g_3(y)), f(x, y)\rangle$. Again, I is a Gröbner basis of I for $\prec_{lex}$.
Remark that as $\gcd(p_1, p_2) = 1$, there exists u, v such that :

$$up_1 + vp_2 = 1$$

We will first prove that $I_1 \cap I_2 \subseteq \langle \text{lcm}(h_1, h_2)(y), \gcd(h_1, h_2)(x - g_3(y)), f(x, y)\rangle$.
Let $f \in I_1$ and $f \in I_2$. We can write f as :

$$f = \sum_{i=1}^{n} m_i$$

Where all the m_i are in $I_1 \cap I_2$.
Let m be any of the m_i. There a few possible cases for m :

- m is purely in y. The smallest polynomial in y belonging to $I_1 \cap I_2$ is by definition $\text{lcm}(h_1, h_2)$. Hence $m \in I$.
- m is a multiple of $(x - g_1)$ and $(x - g_2)$. Now, we don't have the assumption that all the points $p_{0,\dots,d-1,d,\dots,e-1}$ are distinct. Then, we can only interpolate the y_i that are distinct to define $x - g_3$. So to take into account the points skipped during the interpolation, m also needs to be a multiple of α. So we have that $m = k \cdot \alpha(x - g_3)$, thus $m \in I$.
- m is a multiple of h_1 and $x - g_2(y)$. We get that $m = p_1\alpha(x - g_2)$. If we divide m by $\alpha(x - g_3)$, we get :

  $$q = \alpha p_1, r = \alpha p_1(g_2 - g_3)$$

  We can remark that :

  $$\begin{aligned} r &= 0 && \pmod{p_1} \\ r &= \alpha p_1(g_2 - g_2) && \pmod{p_2} \\ r &= 0 && \pmod{p_2} \end{aligned}$$

  Thus by the CRT, $r = 0 \pmod{h_1 h_2}$, so by Theorem 4.1, $m \in I$
- This point is the same as the last one, we only need to swap h_1 with h_2 and $x - g_2(y)$ with $x - g_1(y)$.

Conversly, let us show that $\langle \text{lcm}(h_1, h_2)(y), \gcd(h_1, h_2)(x - g_3(y)), f(x, y)\rangle \subseteq I_1 \cap I_2$.

- It is straightforward that $\langle \text{lcm}(h_1, h_2)\rangle \subseteq I_1 \cap I_2$, as h_1 and h_2 divide $\text{lcm}(h_1, h_2)$.
- Then, we will show that $\langle \alpha(x - g_3(y))\rangle \subseteq I_1 \cap I_2$. Recall that we have $up_1 + vp_2 = 1$. Using the CRT, we have :

  $$x - g_3 = (x - g_2)up_1 + (x - g_1)vp_2$$

  If we multiply by α, we get :

  $$\alpha(x - g_3(y)) = \alpha p_1(x - g_2)u + \alpha p_2(x - g_1)v$$

  Thus we get that $\langle \alpha(x - g_3(y))\rangle \subset I_1 \cap I_2$ as it is an algebraic combination of terms belonging to $I_1 \cap I_2$.
- Finally, let us show that $f(x, y) \subseteq I_1 \cap I_2$. As $\gcd(p_1p_2, \alpha) = 1$, the following equality stands :

  $$u'p_1p_2 + v'\alpha = 1$$

  The CRT formula gives us that :

  $$\begin{aligned} f &= (x - g_1)(x - g_2)p_1p_2u' + \alpha(x - g_3)v' \\ &= (x - g_1)(x - g_2)p_1p_2u' + \alpha((x - g_2)up_1 + (x - g_1)vp_2)v' \end{aligned}$$

  The 2 terms of the expression are clearly in $I_1 \cap I_2$.

As all the generators of I are in $I_1 \cap I_2$, we can conclude that $I \subseteq I_1 \cap I_2$. □

Theorem 5.3. *Let $n = \max(\deg(h_1), deg(h_2))$. The complexity of computing the intersection of two ideals using Theorem 5.2 is $\mathcal{O}(n^2)$. It could be improved using fast algorithms such as fast polynomial division and multiplication.*

Proof. The computation of the Gröbner basis consists in multiplying polynomials and solving 2 CRT systems. These operations can all be done in $\mathcal{O}(n^2)$, hence the total complexity. □

Example 5.1. *Let describe one computation using Theorem 5.2,*
We take $I_1 = \langle y^2 + 2y - 3, x - y + 1\rangle$ and $I_2 = \langle y^2 + 3y - 4, x - y + 3\rangle$
We can factor h_1 and h_2 and get : $h_1 = (y+3)(y-1)$ and $h_2 = (y+4)(y-1)$
Clearly, $\gcd(h_1, h_2) = (y-1)$
We have the following CRT :

$$\begin{cases} f_1 = x - y + 1 \pmod{p_1} = x + 5 \pmod{p_1} \\ f_1 = x - y + 3 \pmod{p_2} = x + 6 \pmod{p_2} \end{cases}$$

Using the CRT we have $f_1 = x - 3y - 5$ (By using the function gcdex to obtain the cofactors)
We then multiply f_1 by $y - 1$ and we obtain the 2nd polynomial of the grobner base which is :

$$(y-1)(x-3y-5) = xy - 3y^2 - x - 2y + 5$$

We then compute the last polynomial of the base using again the CRT :

$$\begin{cases} f_2 = x - 3y - 5 \pmod{(y+3)(y+4)} \\ f_2 = (x-y+3)(x-y+1) \pmod{y-1} = x(x+2) \pmod{y-1} \end{cases}$$

we obtain $f_2 = x^2 - 5y^2 + 2x - 8y + 13$ The the result is then

$$I_1 \cap I_2 = \langle (y-1)(y+4)(y+3),\ (y-1)(x-3y-5),\ x^2 - 5y^2 + 2x - 8y + 13\rangle$$

How can we generalize this process for an intersection of N ideal instead of only 2 ? Let assume we have N Ideal with the same structure which are :

$$I_1 = \langle h_1(y), x - g_1(y)\rangle$$
$$I_2 = \langle h_2(y), x - g_2(y)\rangle$$
$$\dots$$
$$I_N = \langle h_N(y), x - g_N(y)\rangle$$

Also, we have the assumption that:

$$gcd(h_1, \dots, h_N) \neq 1\ \forall i \in \{1, \dots, N\}$$

and

$$gcd(h_i, h_{i+1}) = gcd(h_{i+1}, h_{i+2})\ \forall i \in \{1, \dots, N-2\}$$

We define the polynomials $y_1, \dots, y_N$ such that $y_1 = \dfrac{h_1}{\gcd(h_1, \dots, h_N)}, \dots, y_N = \dfrac{h_N}{\gcd(h_1, \dots, h_N)}$. We want to find f such that :

$$\begin{cases} f_1 = x - g_1 \pmod{y_1} \\ f_1 = x - g_2 \pmod{y_2} \\ \quad\vdots \\ f_1 = x - g_N \pmod{y_N} \end{cases}$$

f_1 can be computed using the CRT. Now, we want to find f_2 such that :

$$\begin{cases} f_2 = f_1 \pmod{\prod_{i=1}^N y_i} \\ f_2 = \prod_{i=1}^N (x - g_i) \pmod{\gcd(\{h_i\})} \end{cases}$$

Again, such a polynomial can be computed using the CRT.

Theorem 5.4. *When* $gcd(h_1, \ldots, h_N) \neq 1 \ \forall i \in \{1, \ldots, N\}$ *and* $gcd(h_i, h_{i+1}) = gcd(h_{i+1}, h_{i+2}) \ \forall i \in \{1, \ldots, N-2\}$

$$I_1 \cap I_2 \cap \cdots \cap I_N = \langle lcm(\{h_i\}), gcd(\{h_i\}) f_1, f_2 \rangle$$

From this reasoning we get the following iterative algorithm :

Algorithm 2 Intersect1$(I_1, \ldots, I_N)$

Input : N Ideals $I_1, \ldots, I_N$ as described above
Output : $I_1 \cap \cdots \cap I_N$

$H \coloneqq \{h_1, .., h_N\}$
$P1 \coloneqq LCM(H)$
$h^* \coloneqq GCD(H)$
$Y \coloneqq \{y_1 = \frac{h_1}{h^*}, \ldots, y_N = \frac{h_N}{h^*}\}$
$X \coloneqq \{x_1 = \frac{x - g_1}{y_1}, \ldots, x_N = \frac{x - g_N}{y_N}\}$
$x^* \coloneqq \prod_{i=1}^{N} \frac{x - g_i}{h^*}$
$c \coloneqq CRT(X, Y)$
$P2 \coloneqq c[1] * h^*$ ▷ The CRT algorithm implemented return 2 elements the first one is the found polynomial and the second one the multiplication of each divisor $\prod_{i=1}^{N} y_i$
$P3 \coloneqq CRT(\{c[1], x^*\}, \{c[2], h^*\})$
return P1,P2,P3

Proposition 5.5. *The complexity of the above algorithm is in* $\mathcal{O}(N * n^2)$

Example 5.2. *We take* $I_1 = \langle y(y-1), x - y + 1 \rangle$, $I_2 = \langle y(y+1), x - y + 2) \rangle$, $I_3 = \langle y(y+2), x - y + 3) \rangle$ *We first compute the gcd of* h_1, h_2 *and* h_3 *wich is clearly y.* $P_1 = lcm(h1, h2, h3) = y(y-1)(y+1)(y+2)$ *we have the first CRT :*

$$\begin{cases} f_1 = x - y + 1 \pmod{y-1} = x \pmod{y-1} \\ f_1 = x - y + 2 \pmod{y+1} = x + 3 \pmod{y+1} \\ f_1 = x - y + 3 \pmod{y+2} = x + 5 \pmod{y+2} \end{cases}$$

We obtain $f_1 = \dfrac{y^2 + 6x^2 - 9y + 8}{6}$

$P_2 = gcd(h1, h2, h3) \cdot f_1 = \dfrac{y(y^2 + 6x^2 - 9y + 8)}{6}$

And then $x^\star$ *is :*

$$\begin{aligned} x^* &= (x - y + 1) * (x - y + 2) * (x - y + 3) \pmod{y} \\ &= (x+1)(x+2)(x+3) \pmod{y} \\ &= x^3 + 6x^2 + 11x + 6 \pmod{y} \end{aligned}$$

We have another CRT :

$$\begin{cases} f_2 = x^* \pmod{y} & = x^3 + 6x^2 + 11x + 6 \pmod{y} \\ f_2 = f_1 \pmod{\dfrac{h_1 h_2 h_3}{y}} & = y^2 + 6x^2 - 9y + 8 \pmod{(y-1)(y+1)(y+2)} \end{cases}$$

We obtain $f_2 = x^3 - 5y^3 + 6y^2 - 3y^2 + 11x + 2y + 6$ *We obtain*

$$\langle y(y-1)(y+1)(y+2), \ \frac{y(y^2 + 6x^2 - 9y + 8)}{6}, \ x^3 - 5y^3 + 6y^2 - 3y^2 + 11x + 2y + 6 \rangle$$

Ideals Intersections case 2

Let us now assume that we have :

$$gcd(h_1, \ldots, h_N) \neq 1$$

But this time we don't necessarily have the following proprieties :

$$gcd(h_1, h_2) = gcd(h_2, h_3) = \cdots = gcd(h_{N-1}, h_N)$$

Which implies that there exist i such that $gcd(h_i, h_{i+1}) \neq gcd(h_{i+1}, h_{i+2})$
This mean that the polynomial $H = \prod_{i=1}^{N} h_i$ has at least one factor which isn't $\gcd(h_1, \ldots, h_N)$ with multiplicity greater than one.
We can then write H as :

$$H = \prod_{k_i \in \mathbb{N}\setminus\{0\}, y_i \in \mathbb{K}} (y - y_i)^{k_i}$$

We define the set H_j as following :

$$H_j = \{\ (y - y_i) \mid k_i \geq j\ \}$$

We define the height of H as follows :

$$height(H) = \max_{k_i}\left(\frac{H}{gcd(h_1, \ldots, h_N)}\right)$$

Let define $W_x = H_x - H_{x+1}$ and $C_w = \{\ (x - g_i) \mid \text{w divide } h_i,\ \forall i \in \{1, \ldots, N\}\}$
We finally define the polynomials $\forall i \in \{1, \ldots, height(H)\}, \forall w \in W_i$:
Case $i = 1$

$$\{f_i = \prod_{c \in C_w} c \pmod{w}\}$$

Case $i > 1$

$$\begin{cases} f_i = \prod_{c \in C_w} c \pmod{w} \\ f_i = f_{i-1} \pmod{\prod_{w^* \in W_{i-1}} w^*} \end{cases}$$

for both cases, we can find f_i using the CRT.

Conjecture 5.1. *The Gröbner basis formed by the intersection of the ideal $I_1, \ldots, I_N$ with the above proprieties is of dimension height(H) + 2.*

Theorem 5.5. *When $gcd(h_1, \ldots, h_N) \neq 1$ and $\exists i$ s.t $gcd(h_i, h_{i+1}) \neq gcd(h_{i+1}, h_{i+2})$*

$$I_1 \cap I_2 \cap \cdots \cap I_N = \langle lcm(h_1, \ldots, h_N), (\prod_{m \in H_2} m) f_1, (\prod_{m \in H_3} m) f_2), \ldots, (\prod_{m \in H_{height(H)}} m) f_{height(H)-2}, f_{height(H)-1})\rangle$$

With this reasoning we can deduce an algorithm to compute the intersection of N ideals with above proprieties.
The algorithm use a "correspondence" list C, this list act like a dictionary which map $y - y_i$ with the resulted multiplication $\prod_{c \in C_i^w} c$.
The function ListOfFactorsAndMultiplicities is also a dictionary, matching each factor with their multiplicities.
The function DecreaseAllMultiplicitiesByOne simply decrease each multiplicities by one, this function act like W_x defined above.

Algorithm 3 Intersect2 $(I_1, \ldots, I_N)$

Input : N Ideals $I_1, \ldots, I_N$ as described above
Output : $I_1 \cap \cdots \cap I_N$

$H \coloneqq \{h_1, .., h_N\}$
$P \coloneqq []$
$C \coloneqq$ Correspondences(h_i, g_i) ▷ List acting as the dictionary defined above
$P[1] \coloneqq LCM(H)$
$H \coloneqq \prod_{i=1}^{N} h_i$
$F \coloneqq$ListOfFactorsAndMultiplicities(H)
$F \coloneqq$DecreaseAllMultiplicitiesByOne(F)
if only one factor has a multiplicity greater than 0 **then**
  return Intersect1$(I_1, \ldots, I_N)$
end if
$Last\_used\_poly\_y \coloneqq 1$
$Last\_found\_poly\_x \coloneqq 1$
$Nb\_It \coloneqq MaxMultiplicity(F)$ ▷ MaxMultiplicity act like the function height() defined above
for j from 1 to Nb_It **do**
  $y^* \coloneqq \prod_{f \in H_j} f$ ▷ All the factor of H with multiplicities greater or equal to j
  $p_y \coloneqq \frac{\frac{P[1]}{y^*}}{last\_used\_poly\_y}$ ▷ Equivalent of W_j but instead of a set of factor, all the factor are multiplied
  $X, Y \coloneqq$ BuildCRTParameters(p_y, C)
  $res \coloneqq$ CRT(X, Y)
  if $i > 1$ **then**
    $res \coloneqq$ CRT$([res[1], last_found_poly_x], [res[2], last_used_poly_y])$
  end if
  $P[i+1] \coloneqq$ NormalForm$(res[1] * y^*, P)$
  $F \coloneqq$ DecreaseAllMultiplicitiesByOne(F)
end for
$X, Y \coloneqq$ BuildCRTParameters$(GCD(h_1, \ldots, h_N), C)$
res $\coloneqq$ CRT$(X, Y \cup \{last_used_poly_y\}$
P[Nb_It+2] $\coloneqq$NormalForm$(res[1], P)$
return P

Proposition 5.6. *The complexity of the above algorithm is in* $\mathcal{O}(n^2(height(H) + N))$

Example 5.3. *We take* $I_1 = \langle y(y-1)(y+1), x-y+1\rangle$, $I_2 = \langle y(y+1)(y-1), x-y+2)\rangle$, $I_3 = \langle y(y+2), x-y+3)\rangle$
We compute $H = y^4(y-1)^2(y+1)^2(y+2)$ *and we deduce that the Height of H is 2, so the obtained intersection is of dimension 4.*
$P_1 = lcm(h1, h2, h3) = y(y-1)(y+1)(y+2)$
$i = 1$
$W_1 = H_1 - H_2 = \{y, y-1, y+1, y+2\} - \{y, y-1, y+2\} = \{y+2\}$
$C_{y+2} = \{x-y+3\}$
We obtain :

$$f1 = x - y + 3 \pmod{y+2} = x + 5 \pmod{y+2}$$

which mean we have $P_2 = y(y+1)(y-1)(x+5)$
$i = 2$
$W_2 = H_2 - H_3 = \{y, y-1, y+1\} - \{y\} = \{y-1, y+1\}$
We obtain the system :

$$\begin{cases} f_2 = f_1 \pmod{y+2} \\ f_2 = (x-y+1)(x-y+2) \pmod{y-1} \\ f_2 = (x-y+1)(x-y+2) \pmod{y+1} \end{cases}$$

Using the CRT we get $f_2 = 3x^2 - 6xy + y^2 + 9x - 9y + 8$
Which mean we have $P_3 = y(\frac{3x^2 - 6xy + y^2 + 9x - 9y + 8}{3})$
We finally have one last CRT :

$$\begin{cases} f_3 = f_2 \pmod{y+2} \\ f_3 = (x-y+3)(x-y+1)(x-y+2) \pmod{y} \end{cases}$$

Which give us $f_3 = x^3 - 3x^2 + 6x^2 - 3xy - 3y^2 + 11x - 3y + 6$.
The final result is :

$$\langle y(y-1)(y+1)(y+2),\ y(y+1)(y-1)(x+5),\ y(\frac{3x^2 - 6xy + y^2 + 9x - 9y + 8}{3}),\ x^3-3x^2+6x^2-3xy-3y^2+11x-3y+6 \rangle$$

6 Conclusion

In this project, we have delved into the foundations of Gröbner bases, a powerful mathematical tool utilized for solving polynomial systems and demonstrating polynomial membership within an ideal. Our research has primarily focused on the latter aspect, specifically exploring the membership of polynomials in ideals and investigating the structure of Gröbner bases for intersections of ideals with specific properties.

Through these investigations, we have gained insights into how the structure of these bases varies based on the parameters of the input ideals. This exploration has been exceptionally enriching since the Gröbner basis generates the resulting ideal of the intersection.

Nevertheless, the structures we have examined are not exhaustive in nature. For instance, what happens if we replace

$$I_1 = \langle h_1(y), x - g_1(y) \rangle, I_2 = \langle h_2(y), x - g_2(y) \rangle$$

with

$$I_1 = \langle h_{1,1}(y), h_{1,2}(y), h_{1,1}(y)(x - g_{1,0}(y)), x^2 - xg_{1,2}(y) - g_{1,1}(y) \rangle$$
$$I_2 = \langle h_{2,1}(y), h_{2,2}(y), h_{2,1}(y)(x - g_{2,0}(y)), x^2 - xg_{2,2}(y) - g_{2,1}(y) \rangle$$

where $\gcd(h_{1,1}, h_{1,2}, h_{2,1}, h_{2,2}) = 1$?
Or with

$$I_j = \langle h_{j,1}(y), h_{j,2}(y), h_{j,1}(y)G_{j,1}(x, y), G_{j,2}(x, y) \rangle$$

with $LT_{\prec_{lex}}(G_{j,2}(x, y))$ parametrized in x and $G_{j,2}(x, y) \in \langle G_{j,1}, h_{j,2} \rangle$ for $j \in \{1, 2\}$ or $j \in \{1, 2, 3\}$? Additionally, how does the scenario unfold when we move beyond two variables and venture into the realm of three, four, or even n variables?

These unanswered questions and unexplored scenarios provide intriguing avenues for further research and deepen our understanding of the complexities associated with Gröbner bases. They inspire future investigations into the impact of varying structures and the behavior of systems with an increased number of variables.

By acknowledging these remaining areas of inquiry, we recognize the potential for continued advancement in this field and open the door to exciting possibilities for future exploration.

References

[1] D. A. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms (third edition)*. Springer-Verlag New-York, 2007.

[2] E. Becker, T. Mora, M.G. Marinari, and C. Traverso. "The shape of the shape lemma". In: *Proceedings ISSAC* (1994).

[3] L. Bernardin, P. Chin, P. Demarco, K. O. Geddes, D. E. G. Hare, K. M. Heal, G. Labahn, J. Mccarron, M. B. Monagan, D. Ohashi, and S. M. Vorkoetter. *Maple programming guide*. 1996.