Modular algorithms for the geometry of rational maps

Hobihasina Patrick RAKOTOARISOA (hobihasina@aims.ac.za)
African Institute for Mathematical Sciences (AIMS)

Supervised by: Dr. Magdaleen Marais
University of Pretoria, South Africa

Co-supervised by: Dr. Janko Böhm and Dr. Dirk Basson
University of Kaiserslautern, Germany
University of Stellenbosch, South Africa

14 May 2020

Submitted in partial fulfillment of a structured masters degree at AIMS South Africa

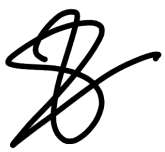
Abstract

This study investigates a modular algorithm for computing the image of a rational map between projective varieties over the rationals. Computations are done in polynomial rings over prime fields. Then, the Chinese remainder theorem is used to obtain one result modulo the product of the primes.
Afterwards, the error tolerant reconstruction reconstitutes the answer over the rational numbers. This approach is probabilistic depending on the primes used but shows significantly better performance than the direct calculation over the rationals in the case where problematic coefficients growth occurs in the intermediate computations.

Key words : modular algorithms, rational maps, projective varieties, Chinese remainder theorem, prime fields, the error tolerant reconstruction.

Declaration

I, the undersigned, hereby declare that the work contained in this research project is my original work, and that any work done by others or by myself previously has been acknowledged and referenced accordingly.



Hobihasina Patrick RAKOTOARISOA, 14 May 2020

Contents

1. Introduction

The interest in rational maps between algebraic sets comes from birational geometry in which two algebraic varieties are equivalent if there is a birational map between them.

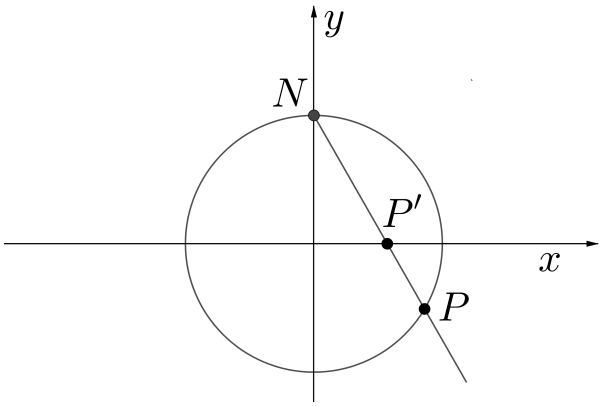


Figure 1.1: The circle and the line are birationally equivalent by stereographic projection

Rational maps are used in handling blowups, parametrization of rational curves, and parametrization of rational surfaces which again are used in applied fields like robotics and computer-aided design. Theoretical applications are the Mori minimal program and the problem of resolution of singularities via iterated blowups called Hironaka's method.

Our study is focusing on computing the image of rational maps which is the fundamental question in the geometry of rational maps. We use the Gröbner basis approach. For an introduction to the subject see (Cox et al., 2015), and see (paraplanecurves.lib) for some implementations. In many applications, computations are over $\mathbb{Q}$ while the theory is considered over $\mathbb{C}$. Indeed, in Gröbner basis computations, a rational polynomial input gives a rational polynomial output. Over $\mathbb{Q}$, intermediate coefficient growth slows down the computation. That is, we have large intermediate results which are much larger than the end result. One way to remedy this is a modular approach. We compute over several prime fields and use the Chinese remainder theorem and rational reconstruction (Kornerup and Gregory, 1983). A classical application is the computation of Gröbner bases, see (Arnold, 2003). In this advanced algorithm, bad primes often cannot be detected effectively, but error tolerant rational reconstruction solves this problem as long as there are only finitely many bad primes, see (Boehm et al., 2015). This is the case if we rely on Gröbner basis methods.

In this thesis, we develop a modular algorithm to compute the image of a rational map. Moreover, we provide an implementation of the algorithms using the computer algebra system Singular in the library modimage.lib, see (Bitbucket, modimage.lib).

The work is divided into five chapters. Chapter 2 discusses rational reconstruction including the error tolerant version. Chapter 3 describes how to apply this to algorithms in commutative algebra dealing with polynomial data. Chapter 4 gives the theoretical background and the algorithm for computing an image of a rational map, Chapter 5 develops the modular algorithm for this problem. Chapter 6 gives timings. We observe the modular approach performs significantly better than direct computation over $\mathbb{Q}$.

2. Rational reconstruction

Rational reconstruction is an important concept of mathematics because it connects calculations over the rational $\mathbb{Q}$ and calculations over the quotient ring $\mathbb{Z}/N\mathbb{Z}$ for an integer $N \geq 2$.
First, integer reconstruction will be discussed to fully understand the concept. Then, we will look at rational reconstruction via Farey map and also via error tolerant reconstruction.

2.1 Reconstruction of integers

Let $N \in \mathbb{N}$. The restriction of the canonical maps $\pi_N : \{x \in \mathbb{Z} \; ; -\frac{N}{2} < x \leq \frac{N}{2}\} \longrightarrow \mathbb{Z}/N\mathbb{Z}$, $\pi_N(x) = \overline{x}$ is bijective. So we can define $\pi_N^{-1}(\overline{x}) \in \mathbb{Z}$ as a reconstruction of $\overline{x} \in \mathbb{Z}/N\mathbb{Z}$ provided that N is sufficiently large. The Chinese remainder theorem is useful to get a large modular result.

2.1.1 Theorem (Chinese remainder theorem in $\mathbb{Z}$)**.** *If $n_1, n_2, \ldots, n_r \in \mathbb{N}$ are pairwise coprime, the ring homomorphism*

$$\begin{array}{rccc} \phi: & \mathbb{Z} & \longrightarrow & \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z} \\ & x & \longmapsto & (\overline{x}, \overline{x}, \ldots, \overline{x}) \end{array}$$

is surjective. Moreover, we have the ring isomorphism

$$\mathbb{Z}/n_1 n_2 \cdots n_r\mathbb{Z} \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}.$$

2.1.2 Remark. The isomorphism in Theorem 2.1.1 means that we can lift modular results to a more large one and we can use this lift to reconstruct integers.

2.1.3 Algorithm. Combining the map π_N and the Chinese remainder theorem, we get a method to reconstruct integers.

Algorithm Reconstruction of integer x

Input: Tuples $(x_1, n_1), (x_2, n_2), \ldots, (x_n, n_r) \in \mathbb{Z} \times \mathbb{N}$ such that $x \equiv \overline{x_i} \pmod{n_i}$, n_i are pairwise coprime and a way to verify the correctness of the result.

Output: integer x.

1: Use the Chinese remainder isomorphism

$$\mathbb{Z}/N\mathbb{Z} \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$$

with $N = n_1 n_2 \cdots n_r$ to lift the modular result to $\mathbb{Z}/N\mathbb{Z}$.

2: Compute a reconstruction of the lift in $\mathbb{Z}/N\mathbb{Z}$ using the map π_N.

3: Verify the result.

2.1.4 Example. Reconstruct $x = 9 \in \mathbb{Z}$ from the modular system

$$\begin{aligned} x &\equiv 4 \pmod{5} \\ x &\equiv 2 \pmod{7}. \end{aligned}$$

The lift in $\mathbb{Z}/35\mathbb{Z}$ is $\overline{9}$ and $\pi_{35}^{-1}(\overline{9}) = 9$ which is correct.
Now if we use

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 0 \pmod 3. \end{aligned}$$

We get $\overline{3}$ as a lift in $\mathbb{Z}/6\mathbb{Z}$ and $\pi_6^{-1}(\overline{3}) = 3$. The reconstruction is wrong. This means that the modular input is not sufficiently large to reconstruct the integer x.

2.2 Farey map

The Chinese remainder theorem showed that we can reconstruct an integer from its modular values. The rational reconstruction extends the concept to lift the modular results over $\mathbb{Q}$.

2.2.1 Definition. For $x = \frac{a}{b} \in \mathbb{Q}$ and $N \in \mathbb{N}$ with $\gcd(b, N) = 1$, we define the residue class modulo N of x as

$$x_N = \overline{a} \cdot \overline{b}^{-1} \in \mathbb{Z}/N\mathbb{Z}.$$

2.2.2 Example. Take $x = \frac{8}{7}$ and $N = 2 \cdot 3 \cdot 5 \cdot 103 = 3090$, we get $x_N = \overline{8} \cdot \overline{883} = \overline{884}$.

Now we want to reconstruct $\frac{8}{7}$ from $\overline{884}$ in Example 2.2.2. The first approach is given by (Kornerup and Gregory, 1983) starting from an injective map between a subset of $\mathbb{Q}$ and a subset of $\mathbb{Z}/N\mathbb{Z}$.

2.2.3 Theorem (Farey map). *Let $N \in \mathbb{N}$. The map*

$$\begin{aligned} \varphi_N : \left\{ \frac{a}{b} \in \mathbb{Q} \;\middle|\; \begin{array}{l} \gcd(a,b) = 1 \\ \gcd(b,N) = 1 \end{array} \; |a|, |b| \leq \sqrt{(N-1)/2} \right\} &\longrightarrow \mathbb{Z}/N\mathbb{Z} \\ \frac{a}{b} &\longmapsto \overline{a} \cdot \overline{b}^{-1} \end{aligned}$$

is injective.

Proof. See (Kornerup and Gregory, 1983). □

2.2.4 Algorithm. If $\overline{r} \in \mathrm{im}(\varphi_N)$, the preimage of $\overline{r}$ gives a reconstruction over $\mathbb{Q}$. Moreover, we can compute this preimage using the algorithm below from (Kornerup and Gregory, 1983).

Algorithm Farey preimage

Input: Integers $0 \leq r \leq N-1$ and $N \geq 2$.
Output: the preimage of $\overline{r}$ respecting φ_N or `false` if $\overline{r}$ is not in the image of φ_N.

1: $(a_0, b_0) := (N, 0)$, $(a_1, b_1) := (r, 1)$, $i = -1$
2: **while** $2a_{i+2}^2 > N - 1$ **do**
3: $\quad i := i + 1$
4: $\quad$ Let q_i the quotient of the Euclidian division of a_i by a_{i+1}
5: $\quad (a_{i+2}, b_{i+2}) = (a_i, b_i) - q_i \cdot (a_{i+1}, b_{i+1})$
6: **end while**
7: **if** $2b_{i+2}^2 \leq N - 1$ **and** $\gcd(a_{i+2}, b_{i+2}) = 1$ **then**
8: $\quad$ **return** $\frac{a_{i+2}}{b_{i+2}}$
9: **end if**
10: **return** `false`

See (Bitbucket, modimage.lib) for the implementation using Singular.

2.2.5 Remark.

- In Algorithm 2.2.4, we have $\left(\frac{a_i}{b_i}\right)_N = \overline{r}$ for all $1 \leq i$, it is an invariant.
- The Algorithm 2.2.4 will terminate because a_i is strictly decreasing.

2.2.6 Example. Reconstruct $\frac{8}{7}$ in Example 2.2.2 using Singular.

```
> ring r = 0, x, dp;
> FareyPreimage(884,3090);
8/7
```

2.3 Error tolerant reconstruction

A second tentative of reconstruction is presented in (Boehm et al., 2015). It is known to tolerate errors and reconstruct more rational than the Farey map.

2.3.1 Example. With $N = 16$, Algorithm 2.2.4 can reconstruct only $\overline{r} \in \text{im}(\varphi_N) = \{\overline{0}, \overline{1}, \overline{14}, \overline{15}\}$ where the output is not `false`.

2.3.2 Definition. Let $N \in \mathbb{N}$. Consider the subset $C_N \subset \mathbb{Z}/N\mathbb{Z}$ defined by $\overline{r} \in C_N$ if there exists $u, v, q \in \mathbb{Z}$ such that

(i) $u \geq 0, v \neq 0$ and $\gcd(u, v) = 1$,

(ii) $q \geq 1$ and q divides N,

(iii) $u^2 + v^2 < \frac{N}{q^2}$ and $u \equiv vr \pmod{\frac{N}{q}}$.

2.3.3 Remark. We have the inclusion $\text{im}(\varphi_N) \subset C_N$. Indeed, we take $q = 1$ and $\frac{u}{v}$ the reconstruction related.

In order to compute all the element of C_N, we will study some properties of the lattice

$$\Lambda = \Lambda_{N,r} = \langle (N, 0), (r, 1) \rangle \subset \mathbb{Z}^2$$

where $N, r \in \mathbb{N}$ are fix and $0 \leq r < N$.

2.3.4 Lemma. (Boehm et al., 2015, Lemma 4.2) All $(x, y) \in \Lambda$ with $x^2 + y^2 < N$ are collinear. So $\frac{x}{y}$ defines a unique rational.

2.3.5 Theorem. *(Boehm et al., 2015, Lemma 4.3) Let $N = N'M$ with $\gcd(N', M) = 1$ and $a, b, s, t \in \mathbb{Z}$. If $\overline{r} \mapsto (\overline{s}, \overline{t})$ is the lifting given by the Chinese remainder isomorphism $\mathbb{Z}/N\mathbb{Z} \cong \mathbb{Z}/N'\mathbb{Z} \times \mathbb{Z}/M\mathbb{Z}$ and $a \equiv bs \pmod{N'}$. Then $(aM, bM) \in \Lambda$.*

So if $(a^2 + b^2)M < N'$, Lemma 2.3.4 will give

$$\frac{x}{y} = \frac{aM}{bM} = \frac{a}{b}$$

for all $(x, y) \in \Lambda$ *with* $x^2 + y^2 < N$.

Moreover, if gcd$(a, b) = 1$ *and* (x, y) *is a shortest non zero vector, we have gcd*(x, y) *divides* M.

2.3.6 Remark. With the same notation in Definition 2.3.2, Lemma 2.3.4 implies $\psi_N : C_N \longrightarrow \mathbb{Q}$, $\psi(\overline{r}) = \frac{u}{v}$ is a map since $u^2 + v^2 < N$. Furthermore, Theorem 2.3.5 carries out a way of computing the image $\psi(\overline{r})$ by taking (u, v) the shortest non zero vector in the lattice $\Lambda_{N,r}$ with the condition $u^2 + v^2 < N$. We will use Gauss-Lagrange-Algorithm to find this shortest vector, see (Bremner, 2012) for more details.

2.3.7 Algorithm. (Boehm et al., 2015)

Algorithm Error Tolerant Lifting

Input: Integers $N \geq 2$ and $0 \leq r \leq N - 1$
Output: $\frac{a}{b}$ or `false`

1: $(a_0, b_0) := (N, 0)$, $(a_1, b_1) := (r, 1)$, $i := -1$
2: **repeat**
3: $\quad i = i + 1$
4: $\quad (a_{i+2}, b_{i+2}) = (a_i, b_i) - \left\lfloor \frac{\langle (a_i,b_i),(a_{i+1},b_{i+1}) \rangle}{\|(a_{i+1},b_{i+1})\|^2} \right\rceil (a_{i+1}, b_{i+1})$
5: **until** $a_{i+2}^2 + b_{i+2}^2 \geq a_{i+1}^2 + b_{i+1}^2$
6: **if** $a_{i+1}^2 + b_{i+1}^2 < N$ **then**
7: $\quad$ **return** $\frac{a_{i+1}}{b_{i+1}}$
8: **else**
9: $\quad$ **return** `false`
10: **end if**

where $\lfloor x \rceil$ is the nearest integer to x and $\lfloor n + \frac{1}{2} \rceil = n + 1$ for all $n \in \mathbb{Z}$.
See (Bitbucket, modimage.lib) for the implementation on Singular.

2.3.8 Example. We reconstruct $\frac{8}{7}$ like in Example 2.2.2 and as in Example 2.3.1 where $N = 16$, we obtain

$$\mathrm{im}(\psi_N) = \{\overline{r} \in \mathbb{Z}/N\mathbb{Z} \; ; \; r \neq 4, 8, 12\}.$$

Since working over the finite fields are more simple than an arbitrary ring $\mathbb{Z}/N\mathbb{Z}$, we adopt the following algorithm to reconstruct a rational x.

2.3.9 Algorithm. (Boehm et al., 2015)

Algorithm Rational reconstruction

Input: Tuples $(r_1, p_1), (r_2, p_2), \ldots, (r_n, p_n) \in \mathbb{Z} \times \mathbb{N}$ such that $x_N \equiv \overline{r_i} \pmod{p_i}$ and a way to verify the correctness of the result.

Output: x

1: Use Chinese remainder isomorphism

$$\mathbb{Z}/N\mathbb{Z} \cong \mathbb{Z}/p_1\mathbb{Z} \times \mathbb{Z}/p_2\mathbb{Z} \times \ldots \times \mathbb{Z}/p_n\mathbb{Z}$$

with $N = p_1 p_2 \cdots p_n$ to lift the modular result to $\mathbb{Z}/N\mathbb{Z}$.

2: Compute a reconstruction of the lift in $\mathbb{Z}/N\mathbb{Z}$ using error tolerant Algorithm.

3: Verify the result.

2.3.10 Example. To illustrate Algorithm 2.3.9, we will reconsider the Example 2.2.2 to reconstruct $x = \frac{8}{7}$ using the primes $3, 5, 11$ and 103. Consider the Chinese remainder isomorphism

$$\chi : \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/103\mathbb{Z} \longrightarrow \mathbb{Z}/16995\mathbb{Z}.$$

The residue class of x in $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/103\mathbb{Z}$ is

$$(\overline{8} \cdot \overline{1}, \overline{8} \cdot \overline{3}, \overline{8} \cdot \overline{8}, \overline{8} \cdot \overline{59}) = (\overline{2}, \overline{4}, \overline{9}, \overline{60})$$

and

$$\chi(\overline{2}, \overline{4}, \overline{9}, \overline{60}) = \overline{2429}.$$

The error tolerant algorithm reconstructs $\frac{8}{7}$ from $\overline{2429}$ with the modulus 16995.

Now, assume that we made a mistake instead of getting $(\overline{2}, \overline{4}, \overline{9}, \overline{60})$ we have $(\overline{2}, \overline{0}, \overline{9}, \overline{60})$.
Then

$$\chi((\overline{2}, \overline{0}, \overline{9}, \overline{60})) = \overline{16025}$$

and we reconstruct $\frac{8}{7}$ using the error tolerant algorithm. Since $(8^2+7^2)\cdot 5 < 3\cdot 11\cdot 103$, so Theorem 2.3.5 provides a unique result whatever the value of the congruence modulo 5 input. Note that the Farey preimage returns `false`.

If we change the congruence modulo the prime 103 to $\overline{61}$. We get

$$\chi(\overline{2}, \overline{4}, \overline{9}, \overline{61}) = \overline{3254}.$$

Then we reconstruct the wrong result $-\frac{17}{47}$. In this case, the prime 103 is called a bad prime.

2.3.11 Definition. (Boehm et al., 2015) A prime p is said a bad prime (respecting a fixing input) if the output over $\mathbb{Q}$ does not reduce modulo p to the result modulo p.

3. Modular methods in commutative algebra

A Modular method is a more indirect way of calculation where intermediate computations are done in one or more quotient rings. This offers in some cases a faster algorithm than a direct approach. This chapter will show a general setup of modular algorithm in commutative algebra. We will also give an example of application in Gröbner basis computation.

3.1 Polynomial reconstruction

Rational reconstruction can be used for polynomial over $\mathbb{Q}$ by applying reconstruction to their coefficients.

3.1.1 Definition. Let $f \in \mathbb{Q}[X_1, X_2, \ldots, X_n]$ and $N \geq 2$ an integer such that N is coprime with all the denominator of coefficient of f, the reduction modulo N of f is the polynomial $f_N \in (\mathbb{Z}/N\mathbb{Z})[X_1, X_2, \ldots, X_n]$ obtained from f by reducing all coefficient modulo N. Generally, if $H = \{h_1, h_2, \ldots, h_r\} \subset \mathbb{Q}[X_1, X_2, \ldots, X_n]$, we define the set $H_N = \{(h_1)_N, (h_2)_N, \ldots, (h_r)_N\}$ on the conditions that every $(h_i)_N$ exist.

3.1.2 Example. The reduction modulo $N = 3$ of $f = X^2 + \frac{1}{2}X + 1 \in \mathbb{Q}[X]$ is

$$f_N = X^2 - X + \overline{1} \in \mathbb{Z}/N\mathbb{Z}[X].$$

3.1.3 Definition. Let $N \geq 2$ an integer and $I \subset \mathbb{Q}[X_1, X_2, \ldots, X_n]$ an ideal. The reduction modulo N of I is the ideal

$$I_N = \langle f_N \,|\, f \in I \cap \mathbb{Z}[X_1, X_2, \ldots, X_n] \rangle \subset (\mathbb{Z}/N\mathbb{Z})[X_1, X_2, \ldots, X_n].$$

3.1.4 Remark. Typically, if the ideal $I = \langle f_1, f_2, \ldots, f_r \rangle$ and p a prime number, we don't have $I_p = \langle (f_1)_p, (f_2)_p, \ldots, (f_r)_p \rangle$. A simple example is given by $I = \langle 2x + 2 \rangle \subset \mathbb{Q}[x]$ and $p = 2$ in which $I_p = \langle x + \overline{1} \rangle$ and $\langle \overline{2}x + \overline{2} \rangle = \langle \overline{0} \rangle$. However, the equality holds for all but finitely many primes p and in practice, we will use the ideal

$$\langle (f_1)_p, (f_2)_p, \ldots, (f_r)_p \rangle \subset (\mathbb{Z}/p\mathbb{Z})[X_1, X_2, \ldots, X_n]$$

if all $(f_i)_p$ exist instead of I_p because finitely bad primes don't have an effect in the result using the error tolerant reconstruction. If one of the $(f_i)_p$ is not defined we reject the prime p.

3.1.5 Example. In some circumstances, all prime can be a bad prime. As an example, consider an algorithm of factorization in $\mathbb{Z}[x]$ and $P = x^4 + 1 \in \mathbb{Z}[x]$. From

$$P(x + 1) = x^4 + 6x^3 + 4x^2 + 6x + 2$$

and Eisenstein's criterion, see (Gallian, 2012, Theorem 17.3), the polynomial P is irreducible over $\mathbb{Z}$.

In the other hand, the polynomial P_p is reducible over $\mathbb{Z}/p\mathbb{Z}$ for all prime p. We can prove it as follow.

- If $\overline{-1}$ is a square in $\mathbb{Z}/p\mathbb{Z}$, say $a^2 = \overline{-1}$. Then, we have

$$x^4 + \overline{1} = x^4 - a^2 = (x^2 + a)(x^2 - a).$$

- If $p > 2$ and $\overline{2}$ is a square in $\mathbb{Z}/p\mathbb{Z}$, say $b^2 = \overline{2}$. Then, we get

$$x^4 + \overline{1} = (x^2 + \overline{1})^2 - (bx)^2 = (x^2 + bx + \overline{1})(x^2 - bx + \overline{1}).$$

- If $p > 2$ and $\overline{-1}$ and $\overline{2}$ are not a square in $\mathbb{Z}/p\mathbb{Z}$. Then, the product $\overline{-1} \cdot \overline{2} = \overline{-2}$ is a square, say $c^2 = \overline{-2}$. This follows easily from Legendre symbol. We get

$$x^4 + \overline{1} = (x^2 - \overline{1})^2 - (cx)^2 = (x^2 - cx - \overline{1})(x^2 + cx - \overline{1}).$$

3.1.6 Algorithm. The procedure `ErrorTolerantReconstruction` in (Bitbucket, modimage.lib) reconstructs polynomials or an ideal using the error tolerant Algorithm 2.3.7 with a given integer modulo $N \geq 2$.

3.2 General reconstruction scheme for modular algorithm

Fix $>$ a global ordering in the set of monomials in the variable $\{X_1, X_2, \ldots, X_n\}$ and $I \subset \mathbb{Q}[X_1, X_2, \ldots, X_n]$ an ideal.
For simplification purposes, in this section as in (Boehm et al., 2015), we assume that the ideal I is related to a well defined ideal $U(0) \subset \mathbb{Q}[X_1, X_2, \ldots, X_n]$ and from every reduction ideal I_p is related to a well defined ideal $U(p) \subset (\mathbb{Z}/p\mathbb{Z})[X_1, X_2, \ldots, X_n]$. Moreover, we make the following assumption : *the equality* $U(0)_p = U(p)$ *holds for all but finitely many primes* p.
Let $G(0)$ the unique reduced Gröbner basis of $U(0)$ and $G(p)$ the unique reduced Gröbner basis of $U(p)$. Then, we introduce the following definition in view of saving more information about the unknown Gröbner basis $G(0)$ during the computation.

3.2.1 Definition. (Boehm et al., 2015)

(1) A prime p is called lucky if

   (a) $U(0)_p = U(p)$ and,

   (b) $\mathrm{LM}(G(0)) = \mathrm{LM}(G(p))$ where $\mathrm{LM}(\cdot)$ is the set of the leading monomial.

   Otherwise p is unlucky.

(2) If $\mathcal{P}$ is a finite set of prime. Set

$$N' = \prod_{p \in \mathcal{P} \text{ lucky}} p \quad \text{and} \quad M = \prod_{p \in \mathcal{P} \text{ unlucky}} p.$$

   Then $\mathcal{P}$ is said sufficiently large if $N' > (a^2 + b^2)M$ for all coefficients $\frac{a}{b}$ of polynomials in $G(0)$.

3.2.2 Lemma. (Boehm et al., 2015, Lemma 5.6) If $\mathcal{P}$ is a sufficiently large set of primes then the reduced Gröbner bases $G(p)$ for all $p \in \mathcal{P}$ lift to the reduced Gröbner basis $G(0)$ via Algorithm 3.1.6 .

In general, we cannot know that a set of primes $\mathcal{P}$ is sufficiently large or not. So we adopt the following random method.

3.2.3 Algorithm. (Boehm et al., 2017)

Algorithm Reconstruct ideal

Input: An algorithm to compute $U(p)$ from I_p and a way of verifying that the computed ideal is equals to $U(0)$.

Output: The ideal $U(0)$.

1: Choose a random set of finite prime $\mathcal{P}$.
2: Compute $U(p)$ for all $p \in \mathcal{P}$.
3: Delete primes in $\mathcal{P}$ respecting to a majority vote on $\mathrm{LM}(G(p))$.
4: Use Chinese remainder theorem to lift the result to $U(N)$ where $N = \prod_{p\in\mathcal{P}} p$.
5: Reconstruct $U(N)$ via error tolerant reconstruction and get U.
6: **if** $U_p = U(p)$ for a random prime $p \notin \mathcal{P}$ **then**
7: **if** $U = U(0)$ **then**
8: **return** U.
9: **else**
10: Enlarge $\mathcal{P}$ and repeat from 2.
11: **end if**
12: **end if**

3.2.4 Remark.

(i) Line 3 in Algorithm 3.2.3 means define a equivalence relation on $\mathcal{P}$ by $p \sim q$ if and only if $\mathrm{LM}(G(p)) = \mathrm{LM}(G(q))$ and replace $\mathcal{P}$ with the largest equivalence class.

(ii) Algorithm 3.2.3 terminates if the set of unlucky prime is finite and the correctness is guaranteed by Lemma 3.2.2.

(iii) Algorithm 3.2.3 is parallelizable by computing all $U(p)$ in line 2 at the same time .

3.3 Modular algorithm for Gröbner basis

As Gröbner bases solve ideal membership problem and very useful in computational algebra. We present a modular technique to compute them using the results seen in the previous section. Remark 3.3.1 below assure that we have all assumption made to run the modular algorithm

3.3.1 Remark. Arnold in (Arnold, 2003) defined lucky prime p for computing Gröbner basis with only the condition (1b) in Defintion 3.2.1 and showed in (Arnold, 2003, Theorem 5.12 and Theorem 6.2) that if the ideal I is homogeneous and p is Arnold-lucky, we get a well defined $G(0)_p$ with $G(0)_p = G(p)$. Using homogenization and dehomgenization with a graded monomial ordering, the results hold in the general setup see (Moeller and Mora, 1984) for more details. Moreover, in (Arnold, 2003, Corollary 5.4 and Theorem 5.13), the set of prime unlucky-Arnold is finite.

3.3.2 Algorithm. Since the Gröbner basis $G(0)$ generates the ideal $U(0)$, we can substitute U to I in Algorithm 3.2.3 and obtain an algorithm for computing Gröbner basis of a given ideal I. Moreover, we use Buchberger algorithm to compute $G(p)$ from I_p for all $p \in \mathcal{P}$ and Buchberger criterion for checking the correctness of the result.

3.3.3 Example. Consider the ideal $I = \langle x^2 - 2y, x^3 - 3z\rangle \subset \mathbb{Q}[x, y, z]$. Suppose that we want to compute the reduced Groebner basis of I respecting to degree reverse lexicographical ordering $>_{\texttt{dp}}$ using a modular method. We will use the primes $\mathcal{P} = \{2, 3, 5, 7\}$.
The first step is to compute $G(p)$ for all $p \in \mathcal{P}$, this can be done using Singular and gives the Gröbner bases

$$\begin{aligned} G(2) &= \langle z, x^2\rangle \\ G(3) &= \langle y^2, xy, x^2 + y\rangle \\ G(5) &= \langle y^2 - 2xz, xy + z, x^2 - 2y\rangle \\ G(7) &= \langle y^2 + xz, xy + 2z, x^2 - 2y\rangle. \end{aligned}$$

Then, we have the two equivalence classes $\{2\}$ and $\{3, 5, 7\}$ according to the equivalence relation $\sim$ in Remark 3.2.4 (i). It follows that the output of the majority vote is $\{3, 5, 7\}$. Now we need to lift the result to $G(3 \cdot 5 \cdot 7)$. The Chinese remainder theorem lifts $G(3), G(5)$ and $G(7)$ to

$$G(3 \cdot 5 \cdot 7) = \langle y^2 - 27xz, xy + 51z, x^2 - 2y\rangle.$$

The last step is to reconstruct $G(3{\cdot}5{\cdot}7)$ over $\mathbb{Q}[x, y, z]$ using the procedure `ErrorTolerantReconstruction` in (Bitbucket, modimage.lib). This yields $G = \{y^2 - \frac{3}{4}xz, xy - \frac{3}{2}z, x^2 - 2y\}$. The equality $G_p = G(p)$ for $p = 11$ holds. Then, Buchberger criterion proves that it is a Gröbner basis of I and it is reduced. Note that the choice $\mathcal{P} = \{2, 3, 5\}$ gives $G = \{y^2 - 3xz, xy - \frac{3}{2}z, x^2 - 2y\}$ which is wrong.

4. Constructions from birational geometry

One of the standard approach of modern mathematics to understand mathematical objects is to study map between those objects, in particular maps which conserve interesting properties of the object. For example in group theory, we study group homomorphism which preserves the group operations. This chapter will focus on a map between projectives varietes and especially describe their image.
Projective algebraic geometry uses the projective space $\mathbb{P}^n_K$ over a field K instead of the affine space K^n and we will represent an element of $\mathbb{P}^n_K$ by homogeneous coordinates $(p_0 : \ldots : p_n)$ see (Boehm, 2017, section 3.8) for more details.
We begin with a map between projective spaces.

4.1 Rational maps of projective spaces

4.1.1 Definition. A rational map between projective spaces is a map

$$\Phi = (p_0 : \ldots : p_n) : \mathbb{P}^m_K \dashrightarrow \mathbb{P}^n_K,\ t \mapsto (p_0(t) : \ldots : p_n(t))$$

where the polynomials $p_i \in K[t_0, \ldots, t_m]$ are homogeneous of the same degree.
The domain of definition of Φ is

$$D(\Phi) = \mathbb{P}^m_K \backslash V(p_0, \ldots, p_n)$$

and the image of Φ is

$$\mathrm{im}(\Phi) = \Phi(D(\Phi)).$$

If $V(p_0, \ldots, p_n) = \emptyset$, we say that the rational map Φ is a morphism.
Let $X \subset \mathbb{P}^m_K$ an algebraic set, the map Φ is a parametrization of X if $\overline{\mathrm{im}(\Phi)} = X$.

4.1.2 Remark. A map

$$\mathbb{P}^m_K \dashrightarrow \mathbb{P}^n_K,\ t \mapsto \left(\frac{p_0(t)}{q_0(t)} : \ldots : \frac{p_n(t)}{q_n(t)}\right)$$

where $p_i, q_i \in K[t_0, t_1, \ldots, t_m]$ homogeneous polynomials of the same degree is reduced to a rational map like in Definition 4.1.1 by canceling the denominator by multiplying with $g = \mathrm{lcm}(q_0, q_1, \ldots, q_n)$ and it yields the same map.

4.1.3 Example. Take $K = \mathbb{R}$ and consider the rational map

$$\Phi : \mathbb{P}^1_K \dashrightarrow \mathbb{P}^2_K,\ t \mapsto (t_0^2 + t_1^2 : t_0^2 - t_1^2 : 2t_0t_1).$$

The vanishing locus $V(t_0^2 + t_1^2, t_0^2 - t_1^2, 2t_0t_1) = \emptyset \subset \mathbb{P}^1_K$ because the point $(0, 0)$ is the only zero. Hence $D(\Phi) = \mathbb{P}^1_K$ and Φ is a morphism.
We will see later that

$$\mathrm{im}(\Phi) = V(x_1^2 + x_2^2 - x_0^2) \subset \mathbb{P}^2_K$$

which is the smallest projective algebraic set containing the affine circle $C \subset K^2$. Indeed, we have the equality

$$V(x_1^2 + x_2^2 - x_0^2) = \{(1 : x : y) \mid (x, y) \in C\} \subset \mathbb{P}^2_K.$$

This gives a parametrization of the circle in $\mathbb{P}^2_K$.
Note that this parametrization is different than the usual rational parametrization of the circle in K^2

$$K \to K^2,\ t \mapsto \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$$

by stereographic projection in which we miss the pole point $(-1, 0)$. Whereas in the projective case, the point at infinity $(0 : 1)$ gives as image $\Phi(0 : 1) = (1 : -1 : 0)$.

4.2 Quotients and saturations of ideals

Quotients and saturations play an important role in the correspondence between geometry and algebra. We will recall them in this section.

4.2.1 Definition. Let I and J be ideals in $K[t_1, \ldots, t_n]$.

(i) The quotient of I by J is the ideal

$$I : J = \{f \in K[t_1, \ldots, t_n] \,|\, fg \in I,\ \forall g \in J\}.$$

(ii) The saturation of I by J is the ideal

$$I : J^\infty = \{f \in K[t_1, \ldots, t_n] \,|\, \exists N \in \mathbb{N} : fg^N \in I,\ \forall g \in J\}.$$

The two definitions are related by the following proposition.

4.2.2 Proposition. (Cox et al., 2015) If I, $J \subset K[t_1, \ldots, t_n]$ are ideals. Then

(i) $I : J^\infty = I : J^N$ for all sufficiently large N.

(ii) $\sqrt{I : J^\infty} = \sqrt{I} : J$.

Proof. (i) The inclusion $I : J^\infty \supset I : J^N$ for all $N \in \mathbb{N}$ is straightforward. For the other inclusion, let $f \in I : J^\infty$ and assume $J = \langle g_1, \ldots, g_s\rangle$. There exists $N_i \in \mathbb{N}$ such that $fg_i^{N_i} \in I$ for $i = 1, \ldots, s$.
Set $M = \max\{N_1, \ldots, N_s\}$. We have $fg_i^M \in I$ for $i = 1, \ldots, s$.
As $J^{sM} \subset \langle g_1^M, \ldots, g_s^M\rangle$, we get $fJ^{sM} \subset f\langle g_1^M, \ldots, g_s^M\rangle \subset \langle fg_1^M, \ldots, fg_s^M\rangle \subset I$. This means that $f \in I : J^{sM}$. On the other hand, the ring $K[t_1, t_2, \ldots, t_n]$ is Noetherian, the ascending chain of ideals

$$I \subset I : J \subset I : J^2 \subset I : J^3 \subset \cdots.$$

will stabilize at a certain $N \in \mathbb{N}$. It follows that $f \in I : J^{sM} \subset I : J^N$.
For (ii), the first inclusion $\sqrt{I : J^\infty} \subset \sqrt{I} : J$ is straightforward. For the opposite inclusion, let $f \in \sqrt{I} : J$ and assume $J = \langle g_1, g_2, \ldots, g_s\rangle$. So $fg_i \in \sqrt{I}$. There exists $M \in \mathbb{N}$ such that $f^M g_i^M \in I$. It follows that $f^M J^{sM} \subset I$. This means that $f \in I : J^{sM} = I : J^\infty$ using the proof of (i). Therefore $f \in \sqrt{I : J^\infty}$. □

4.2.3 Remark. The Proposition 4.2.2 leads to an algorithm computing saturations by iterating the ideal quotients until it stabilizes since we have the equality

$$(I : J) : L = I : (J \cdot L)$$

for all ideals I, J and L in $K[t_1, \cdots, t_n]$.

There is a relation between ideal quotients and the Zariski closure of a difference of varieties

4.2.4 Proposition. (Cox et al., 2015) If $I, J \subset K[t_1, \ldots, t_n]$ are ideals, then $\overline{V(I)\backslash V(J)} \subset V(I : J)$ where V is the affine vanishing locus.

Proof. We have to show that $I : J \subset I(V(I)\backslash V(J))$. Let $f \in I : J$ and $p \in V(I)\backslash V(J)$. Then $fg \in I$ for all $g \in J$. As $p \in V(I)$, we obtain $f(p)g(p) = 0$ for all $g \in J$. Since $p \notin V(J)$, for $g \neq 0 \in J$, we have $g(p) \neq 0$. This implies that $f(p) = 0$ for all $p \in V(I)\backslash V(J)$ which means $f \in I(V(I)\backslash V(J))$. Applying V on both sides yields $\overline{V(I)\backslash V(J)} \subset V(I : J)$. □

4.2.5 Example. (Cox et al., 2015) Let $I = \langle x^2(y-1)\rangle$ and $J = \langle x\rangle$ ideal in $\mathbb{C}[x, y]$. A geometric interpretation shows that $\overline{V(I)\backslash V(J)} = V(y-1)$. However, the ideal quotient is

$$\begin{aligned} I : J &= \{f \in \mathbb{C}[x, y] \,;\, fg \in I \ \forall g \in J\} \\ &= \{f \in \mathbb{C}[x, y]; fx \in I\} \\ &= \{f \in \mathbb{C}[x, y] \ ; \ \exists A \in \mathbb{C}[x, y],\ fx = Ax^2(y-1)\} \\ &= \{f \in \mathbb{C}[x, y] \ ; \ \exists A \in \mathbb{C}[x, y],\ f = Ax(y-1)\} \\ &= \langle x(y-1)\rangle. \end{aligned}$$

This example shows that the vanishing locus $V(I : J)$ does not match with $\overline{V(I)\backslash V(J)}$. In order to obtain an equality, we need ideal other than the quotient $I : J$.

4.2.6 Proposition. (Cox et al., 2015) If I, J are ideals in $K[t_1, \ldots, t_n]$ and K is algebraically closed fields, then

$$V(I : J^\infty) = \overline{V(I)\backslash V(J)}.$$

Proof. The inclusion $\overline{V(I)\backslash V(J)} \subset V(I : J^\infty)$ is straightforward using the same argument in Proposition 4.2.4. For the reverse inclusion, we will show first that $I(V(I)\backslash V(J)) \subset \sqrt{I} : J$. Let $f \in I(V(I)\backslash V(J))$ and $g \in J$. We have $fg \in I(V(I))$ because f is vanishing on $V(I)$. Using the affine Nullstellensatz, we get $fg \in \sqrt{I}$ for all $g \in J$. Then $f \in \sqrt{I} : J$ and $I(V(I)\backslash V(J)) \subset \sqrt{I} : J$. Then applying V on both sides yields

$$V(\sqrt{I} : J) \subset V(I(V(I)\backslash V(J))) = \overline{V(I)\backslash V(J)}.$$

Proposition 4.2.2 (ii) gives $\sqrt{I} : J = \sqrt{I : J^\infty}$. It follows that

$$V(I : J^\infty) = V(\sqrt{I : J^\infty}) = V(\sqrt{I} : J) \subset \overline{V(I)\backslash V(J)}.$$

□

The following proposition and theorem lead us to an algorithm for computing quotients and saturations.

4.2.7 Proposition. (Cox et al., 2015) Let I and $J_1, J_2, \ldots J_r$ be ideals in $K[t_1, t_2, \ldots, t_n]$ then

(i) $I : (\sum_{i=1}^r J_i) = \cap_{i=1}^r (I : J_i)$,

(ii) $I : (\sum_{i=1}^r J_i)^\infty = \cap_{i=1}^r (I : J_i^\infty)$.

4.2.8 Theorem. *(Cox et al., 2015) Let $I \subset K[t_1,\dots,t_n]$ an ideal and $g \neq 0 \in K[t_1,\dots,t_n]$. Then*

(i) If $I \cap \langle g\rangle = \langle gf_1, gf_2, \dots, gf_s\rangle$ where $f_i \in K[t_1,\dots,t_n]$, we have $I : \langle g\rangle = \langle f_1,\dots,f_s\rangle$.

(ii) If $I = \langle h_1,\dots,h_s\rangle$ and $\overline{I} = \langle h_1,\dots,h_s, 1-yg\rangle$, we get $I : \langle g\rangle^\infty = \overline{I} \cap K[t_1,\dots,t_n]$.

Proof. For (i), clearly we have

$$g\langle f_1,\dots,f_s\rangle \subset \langle gf_1,\dots,gf_s\rangle = I \cap \langle g\rangle \subset I.$$

So $\langle f_1,\dots,f_s\rangle \subset I : \langle g\rangle$. Now if $f \in I : \langle g\rangle$, then $fg \in I \cap \langle g\rangle$. We can write

$$fg = \sum_{i=1}^{s} a_i g f_i$$

with $a_i \in K[t_1,\dots,t_n]$. It follows that $f = \sum_{i=1}^s a_i f_i$ which means that $f \in \langle f_1,\dots,f_s\rangle$.
For (ii), let $f \in I : \langle g\rangle^\infty$. There exists $N \in \mathbb{N}$ such that $fg^N \in I$. Then we can write $fg^N = \sum_{i=1}^s a_i h_i$ with $a_i \in K[t_1,\dots,t_n]$ and

$$\begin{aligned} f &= y^N f g^N + f - y^N f g^N \\ &= y f g^N + f(1 - y^N g^N) \\ &= y f g^N + f(1 + yg + y^2g^2 + \cdots + y^{N-1}g^{N-1})(1-yg) \\ &= y\sum_{i=1}^{s} a_i h_i + f(1 + yg + y^2g^2 + \cdots + y^{N-1}g^{N-1})(1-yg) \in \overline{I} \end{aligned}$$

If follows that $f \in \overline{I} \cap K[t_1,\dots,t_n]$. For the other inclusion, let $f \in \overline{I} \cap K[t_1,\dots,t_n]$. We have $f = \sum_{i=1}^s a_i h_i + b(1-yg)$ with $a_i, b \in K[t_1,\dots,t_n,y]$. Since f is independent of y, we can substitute $y = \frac{1}{g}$ and get $f = \sum_{i=1}^s a_i(t_1,\dots,t_n,\frac{1}{g})h_i$.
Set $N = \max\{\deg_y(a_i) \mid i = 1,\dots,s\}$. Then $g^N a_i(t_1,\dots,t_n,\frac{1}{g}) \in K[t_1,\dots,t_n]$ and

$$fg^N = \sum_{i=1}^{s} g^N a_i(t_1,\dots,t_n,\frac{1}{g})h_i \in I.$$

Therefore $f \in I : \langle g\rangle^\infty$. □

4.2.9 Algorithm. Let $I, J \subset K[t_1,\dots,t_n]$ ideals such that $J = \langle g_1,\dots,g_s\rangle$.

(i) In order to compute $I : J$, Proposition 4.2.7 implies $I : J = \bigcap_{i=1}^s (I : \langle g_i\rangle)$ and we can get $I : \langle g_i\rangle$ via Theorem 4.2.8 (i). The command `quotient(I:J)` in Singular computes $I : J$.

(ii) Using the same argument as in (i), Theorem 4.2.8 (ii) yields an algorithm for computing saturations. Note that Singular uses the iterative quotient algorithm mentioned in Remark 4.2.3 through the command `sat(I,J)` in the library `elim.lib` and gives as output the ideal $I : J^\infty$ and the smallest $N \in \mathbb{N}$ such that $I : J^\infty = I : J^N$.

4.2.10 Example. In Example 4.2.5, Singular gives $I : J = \langle x^2y - x^2\rangle$ and the saturation $I : J^\infty = \langle y-1\rangle$ with stability index $N = 2$, that is $I : J^\infty = I : J^2$.

4.3 Projective elimination

In view of describing the image of rational map, we introduce an additional tool in the algebra-geometry correspondence. This is elimination of ideal which corresponds to projection in geometry.
First we recall how it appears in the affine case in the following theorem.

4.3.1 Theorem. *(Boehm, 2017) Let $I \subset K[t_1, \ldots, t_n]$ ideal with K an algebraically closed field. Set $A = V(I) \subset K^n$ the vanishing locus of I and let $0 \leq k < n$. Consider*

$$\pi_k : K^n \longrightarrow K^{n-k}, (a_1, \ldots, a_n) \longmapsto (a_{k+1}, \ldots, a_n)$$

be the projection onto the last k components. Then

$$\overline{\pi_k(A)} = V(I_k)$$

where $I_k = I \cap K[t_{k+1}, \ldots, t_n]$ is the elimination ideal of I.

In the projective case, things are more complicated as the following example will show.

4.3.2 Example. Let $I = \langle x + yz, x + xz \rangle \subset \mathbb{C}[x, y, z]$ and $A = V(I) \subset \mathbb{P}^1_{\mathbb{C}} \times \mathbb{C}$. This makes sense because I is homogeneous in the variables x and y. Then it is straightforward to show that

$$V(A) = \{((0:1), 0), ((1:1), -1), ((1:1), -1)\} \subset \mathbb{P}^1_{\mathbb{C}} \times \mathbb{C}.$$

So the image of A under the projection

$$\pi : \mathbb{P}^1_{\mathbb{C}} \times \mathbb{C} \longrightarrow K, \ ((a_1 : a_2), a_3) \longmapsto a_3$$

is $\pi(A) = \{0, -1\}$. If we try to use the affine elimination, we get $I \cap \mathbb{C}[z] = \{0\}$ which means that the image is all $\mathbb{C}$. Indeed, in affine point of view $V(I) \subset \mathbb{C}^2 \times \mathbb{C}$ contains the points $(0, 0, t)$ for every $t \in \mathbb{C}$ but the point $((0:0), t)$ does not exist in $\mathbb{P}^1_{\mathbb{C}} \times \mathbb{C}$.
So the affine elimination does not capture the fact that we are in projective space. However, we can extend it by removing points which are not defined in the projective space.

4.3.3 Definition. Let $I \in K[t_0, t_1, \ldots, t_m, x_1, x_2, \ldots, x_n]$ be an ideal generated by homogeneous polynomials in the variables $t_0, \ldots, t_m$. The projective elimination ideal I of is the ideal

$$\hat{I} = (I : \langle t_0, \ldots, t_m \rangle^\infty) \cap K[x_1, x_2, \ldots, x_n].$$

4.3.4 Example. In Example 4.3.2, we have $\hat{I} = (I : \langle x, y \rangle^\infty) \cap \mathbb{C}[z] = \langle y(y+1) \rangle$ and $\pi(A) = V(\hat{I})$. The following theorem justifies this observation.

4.3.5 Theorem. *(Cox et al., 2015) Let K be an algebraically closed field. Let $I = \langle f_1, \ldots, f_p \rangle \subset K[t_0, \ldots, t_m, x_1, \ldots, x_n]$ be an ideal generated by homogeneous polynomials in the variables $t_0, \ldots, t_m$. We define*

$$V(I) = \{(t, x) \in \mathbb{P}^m_K \times K^n \mid f(t, x) = 0 \text{ for all } f \in I \text{ homogeneous in } t_i\}$$

and

$$\pi : \mathbb{P}^m_K \times K^n \longrightarrow K^n, \ ((t_0 : \ldots : t_m), (x_1, \ldots, x_n)) \longmapsto (x_1, \ldots, x_n).$$

Then

$$\pi(V(I)) = V(\hat{I}).$$

Proof. For the inclusion $\pi(V(I)) \subset V(\hat{I})$, let $f \in \hat{I}$, there exists $s_i \in \mathbb{N}$ such that $ft_i^{s_i} \in I$ for all $i = 0, \ldots, m$. If $(\tilde{t}, \tilde{x}) \in V(I)$, we have

$$f(\tilde{x})\tilde{t}_i^{s_i} = 0.$$

As $\tilde{t} \in \mathbb{P}_K^m$, there exists i such that $\tilde{t}_i \neq 0$. Then we get $f(\tilde{x}) = 0$ for all $f \in \hat{I}$ and $\pi(\tilde{t}, \tilde{x}) = \tilde{x} \in V(\hat{I})$. The other inclusion $\pi(V(I)) \supset V(\hat{I})$ will be proved by contradiction. Assume that $\tilde{x} \in V(\hat{I})$ and $\tilde{x} \notin \pi(V(I))$. Set $L = \langle f_1(t_0, \ldots, t_m, \tilde{x}), \ldots, f_p(t_0, \ldots, t_m, \tilde{x})\rangle$.
The assertion $\tilde{x} \notin \pi(V(I))$ means that for the homogeneous ideal L,

$$V(L) = \emptyset \subset \mathbb{P}_K^m.$$

The projective Nullstellensatz implies that $\sqrt{L} = \langle 1\rangle$ or $\sqrt{L} = \langle t_0, \ldots, t_m\rangle$. If $\sqrt{L} = \langle 1\rangle$, clearly $L = \langle 1\rangle$ and $\langle t_0, \ldots, t_m\rangle^r \subset L$ for all $r \in \mathbb{R}$. If $\sqrt{L} = \langle t_0, \ldots, t_m\rangle$. There exist $r_i \in \mathbb{N}$ such that $t_i^{r_i} \in L$. Set $N = \max\{r_i \ ; \ i = 0, \ldots, m\}$. It follows that

$$\langle t_0, \ldots, t_m\rangle^{mN} \subset \langle t_0^N, \ldots, t_m^N\rangle \subset L.$$

In any case, there exists $r \in \mathbb{N}$ such that $\langle t_0, \ldots, t_m\rangle^r \subset L$. So every monomial t^α of degree $|\alpha| = r$ is in L. We can write

$$t^\alpha = \sum_{i=1}^{p} g_i(t_0, \ldots, t_m) f_i(t_0, \ldots, t_m, \tilde{x})$$

Taking the homogeneous part, we can assume that g_i is homogeneous of degree $|\beta_i| = r - \deg(f_i)$. Writing g_i as a sum of monomial of degree $|\beta_i|$ shows that the set

$$\{t^{\beta_i} f_i(t_0, \ldots, t_m) \mid |\beta_i| = r - \deg(f_i), i = 1, \ldots, p\}$$

spans the vector space of all homogeneous polynomial of total degree r in $t_0, \ldots, t_m$. Since this vector space has finite dimension say N_r. We can pick N_r elements which form a basis

$$\{t^{\beta_i} G_i(t_0, \ldots, t_m, \tilde{x}) \ ; \ i = 1, \ldots, N_r\}$$

with $G_i(t_0, \ldots, t_m, \tilde{x}) \in L$ from $G_i(t_0, \ldots, t_m, x_1, \ldots, x_n) \in I$.
The homogeneous polynomial $G(t_0, \ldots, t_m, x_1, \ldots, x_n)$ has degree r, so we can write it as

$$G_i(t_0, \ldots, t_m, x_1, \ldots, x_n) = \sum_{|\alpha|=r} a_{i,\alpha}(x_1, \ldots, x_n) t^\alpha$$

as a polynomial in $t_0, \ldots, t_m$. Hence we get a square matrix $(a_{i,\alpha}(x_1, \ldots, x_n))_{i,\alpha}$ of polynomials.
Let

$$D(x_1, \ldots, x_n) = \det((a_{i,\alpha}(x_1, \ldots, x_n))_{i,\alpha}).$$

Since $D(\tilde{x}) \neq 0$ because $G_i(t_0, \ldots, t_m, \tilde{x})$ is a basis, we have $D(x_1, \ldots, x_n) \neq 0$.
Now we are going to see that $D(x_1, \ldots, x_n) \in \hat{I}$ which contradicts $D(\tilde{x}) \neq 0$.
Consider the system of equations in Y_α

$$\sum_{|\alpha|=r} a_{i,\alpha}(x_1, \ldots, x_n) Y_\alpha = G_i(t_0, \ldots, t_m, x_1, \ldots, x_n)$$

over the rational function field $K(t_0, \ldots, t_m, x_1, \ldots, x_n)$. Since $D(x_1, \ldots, x_n) \neq 0$. The system has a unique solution which is $Y_\alpha = t^\alpha$. Cramer's Rule can express this solution as

$$t^\alpha = \frac{\det(M_\alpha)}{D(x_1, \ldots, x_n)}$$

where M_α is a matrix obtained from $(a_{i,\alpha}(x_1,\ldots,x_n))_{i,\alpha}$ by replacing the column α by the polynomials

$$G_1(t_0,\ldots,t_m,x_1,\ldots,x_n),\ldots,G_{N_r}(t_0,\ldots,t_m,x_1,\ldots,x_n).$$

If we expand $\det(M\alpha)$ along this column we will get

$$t^\alpha D(x_1,\ldots,x_n)=\sum_{i=1}^{N_r} H_i(x_1,\ldots,x_n)G_i(t_0,\ldots,t_m,x_1,\ldots,x_n)\in I.$$

This means that $D(x_1,\ldots,x_n)\in \hat{I}$. □

4.3.6 Corollary. (Boehm, 2017) If K is algebraically closed field, and $I\subset K[t_0,\ldots,t_m,x_0,\ldots,x_n]$ a bihomogeneous ideal which means homogeneous both in the variables $t_0,\ldots,t_m$ and the variables $x_1,\ldots,x_n$. We can define

$$V(I)=\{(t,x)\in\mathbb{P}^m_K\times\mathbb{P}^n_K \mid f(t,x)=0 \text{ for all bihomogeneous } f\in I\}$$

and

$$\pi:\mathbb{P}^m_K\times\mathbb{P}^n_K\longrightarrow\mathbb{P}^n_K,\ ((t_0:\ldots:t_m),(x_0:\ldots:x_n))\longmapsto(x_0:\ldots:x_n).$$

Then

$$\pi(V(I))=V(\hat{I}).$$

Proof. First of all we need to show that the ideal $\hat{I}\subset K[x_0,\ldots,x_n]$ is homogeneous. Note that the ideal I is a homogeneous ideal of $K[t_0,\ldots,t_m,x_0,\ldots,x_n]$. We recall that

$$\hat{I}=(I:\langle t_0,\ldots,t_m\rangle)\cap K[x_0,\ldots,x_n].$$

Let $f\in\hat{I}$ and write $f=\sum_i f_i$ as sum of homogeneous parts. There are $s_j\in\mathbb{N}$ such that $f\cdot t_j^{s_j}\in I$ for all $j=0,\ldots,m$. Then $\sum_i f_i\cdot t_j^{s_j}\in I$. The expression $\sum_i f_i t_j^{s_j}$ is the decomposition of $ft_j^{s_j}$ as sum of homogeneous parts.
Since I is a homogeneous ideal, each summand $f_i t_j^{s_j}\in I$ for all $j=0,\ldots,m$. This means that each homogeneous summand $f_i\in\hat{I}$ for all $f\in\hat{I}$. This implies that $\hat{I}\subset K[x_0,\ldots,x_n]$ is homogeneous. Then $V(\hat{I})\subset\mathbb{P}^n_K$ is well defined.
Now observe that the ideal I also defines a vanishing locus in $\mathbb{P}^m_K\times K^{n+1}$ because it is homogeneous in $t_0,\ldots,t_m$. Theorem 4.3.5 gives

$$\pi(V(I))=V(\hat{I})\subset K^{n+1}.$$

In the equivalence classes $\mathbb{P}^n_K$, we have

$$\pi(V(I))=V(\hat{I})\subset\mathbb{P}^n_K.$$

□

4.3.7 Remark. The algorithm to compute the elimination ideal $\hat{I}$ needs an elimination ordering for $t_0,\ldots,t_m$ on the monomials of $K[t_0,\ldots,t_m,x_0,\ldots,x_n]$. In our examples, we will always use the product ordering $>$ of $>_{\mathsf{dp}}$ on the monomials t^α in the variables $t_0,\ldots,t_m$ and $>_{\mathsf{dp}}$ on the monomials x^β in the variables $x_0,\ldots,x_n$ defined by

$$t^\alpha x^\beta > t^{\alpha'}x^{\beta'} \Leftrightarrow t^\alpha > t^{\alpha'} \text{ or } (t^\alpha = t^{\alpha'} \text{ and } x^\beta > x^{\beta'}).$$

4.3.8 Example. Let $I = \langle t_0t_1x - t_0^2y, t_1^2x - t_0^2z, t_1^2y - t_0t_1z\rangle \subset \mathbb{C}[t_0, t_1, x, y, z]$. The ideal I is bihomogeneous, so we can define the vanishing locus $V(I) \subset \mathbb{P}^2_{\mathbb{C}} \times \mathbb{P}^3_{\mathbb{C}}$ like in Corollary 4.3.6. The projection of $V(I)$ on the second component $\mathbb{P}^3_{\mathbb{C}}$ is defined by $V(\hat{I})$ with the elimination ideal

$$\hat{I} = (I : \langle t_0, t_1\rangle^\infty) \cap \mathbb{C}[x, y, z] = \langle y^2 - xz\rangle \subset K[x, y, z].$$

This is the equation of the parabola in $\mathbb{P}^2_{\mathbb{C}}$.

4.4 Image of rational map

In the previous section, we have used elimination to describe the image of projection map. Now we will consider an arbitrary rational map. How can we describe the image in terms of homogeneous ideal? The affine case is summarized in the following proposition.

4.4.1 Proposition. (Boehm, 2017) If K is a algebraically closed field and

$$\varphi = \left(\frac{f_1}{g_1}, \frac{f_2}{g_2}, \ldots, \frac{f_n}{g_n}\right) : K^m \dashrightarrow K^n$$

is a rational map of affine spaces with $f_i, g_i \in K[t_1, \ldots, t_m]$. Then

$$\overline{\mathrm{im}(\varphi)} = V(J \cap K[x_1, \ldots, x_n])$$

where

$$J = \langle g_1x_1 - f_1, \ldots, g_nx_n - f_n, 1 - g_1g_2 \cdots g_ns\rangle \subset K[s, t_1, \ldots, t_m, x_1, \ldots, x_n].$$

The ideal J in Proposition 4.4.1 describes the graph of φ by $V(J) \in K^m \times K^n$. We will present the equivalents in projective case.

4.4.2 Lemma. (Boehm, 2017) Let K be an algebraically closed field and

$$\begin{array}{rccc} \Phi : & \mathbb{P}^m_K & \longrightarrow & \mathbb{P}^n_K \\ & t = (t_0 : \ldots : t_m) & \longmapsto & (f_0(t) : \ldots : f_n(t)) \end{array}$$

a morphism with $f_i \in K[t_1, \ldots, t_m]$ homogeneous of the same degree. Then, the graph of the map Φ is

$$\Gamma(\Phi) = V(J) \subset \mathbb{P}^m_K \times \mathbb{P}^n_K$$

where

$$J = \left\langle \mathrm{minors}_2 \begin{pmatrix} x_0 & \cdots & x_n \\ f_0 & \cdots & f_n \end{pmatrix} \right\rangle \subset K[t_0, \ldots, t_m, x_0, \ldots, x_n].$$

Proof. Let $(t, x) \in \Gamma(\Phi)$ with $x = (x_0 : \ldots : x_n) \in \mathbb{P}^n_K$. We have $x = \Phi(t) \in \mathbb{P}^n_K$ which means that the vectors $(x_0, \ldots, x_n)$ and $(f_0(t), \ldots, f_n(t))$ are linearly dependent. It follows that

$$(t, x) \in V(J) \subset \mathbb{P}^m_K \times \mathbb{P}^n_K$$

because all the 2×2 minors generating J are vanishing in this point. We get $\Gamma(\Phi) \subset V(J)$.
For the other inclusion, let $(t, x) \in V(J)$. For all $0 \leq i, j \leq n$, we have

$$x_if_j(t) - x_jf_i(t) = 0.$$

As $x \in \mathbb{P}^n_K$, there exists an $x_i \neq 0$. Furthermore, the rational map Φ is a morphism then there is a $f_j(t) \neq 0$.
So

$$x_j f_i(t) = x_i f_j(t) \neq 0 \quad \text{and} \quad x_i = \frac{x_j}{f_j(t)} f_i(t) \text{ for all } 0 \leq i \leq n \text{ with } \frac{x_j}{f_j(t)} \neq 0.$$

Hence

$$(x_0, \ldots, x_n) = \frac{x_j}{f_j(t)}(f_0(t), \ldots, f_n(t)).$$

This means that $x = (f_0(t) : \ldots : f_n(t))$ in $\mathbb{P}^n_K$. Thus $(t, x) \in \Gamma(\Phi)$ and $V(J) \subset \Gamma(\Phi)$. □

So far, we are able to describe the image of a morphism of projective space.

4.4.3 Theorem. *(Boehm, 2017) Let K be an algebraically closed field and*

$$\begin{array}{rccc} \Phi : & \mathbb{P}^m_K & \longrightarrow & \mathbb{P}^n_K \\ & t = (t_0 : \ldots : t_m) & \longmapsto & (f_0(t) : \ldots : f_n(t)) \end{array}$$

a morphism with $f_i \in K[t_1, \ldots, t_m]$ homogeneous and have the same degree. Then

$$im(\Phi) = V((J : \langle t_0, \ldots, t_m \rangle^\infty) \cap K[x_0, \ldots, x_n])$$

where

$$J = \left\langle minors_2 \begin{pmatrix} x_0 & \cdots & x_n \\ f_0 & \cdots & f_n \end{pmatrix} \right\rangle \subset K[t_0, \ldots, t_m, x_0, \ldots, x_n].$$

Proof. It follows from Lemma 4.4.2 that $V(J) \in \mathbb{P}^m_K \times \mathbb{P}^n_K$ is the graph of the map Φ and projective elimination applied to J represents the projection of the graph $V(J)$ in the second component $\mathbb{P}^n_K$ which is the image of Φ. □

4.4.4 Example. Consider the rational map

$$\begin{array}{rccc} \Phi : & \mathbb{P}^1_{\mathbb{C}} & \longrightarrow & \mathbb{P}^2_{\mathbb{C}} \\ & (t_0 : t_1) & \longmapsto & (t_0^2 : t_0 t_1 : t_1^2). \end{array}$$

It is a morphism. The ideal J describing the graph of Φ is

$$J = \left\langle \text{minors}_2 \begin{pmatrix} x & y & z \\ t_0^2 & t_0 t_1 & t_1^2 \end{pmatrix} \right\rangle = \langle t_0 t_1 x - y t_0^2, t_1^2 x - t_0^2 z, t_1^2 y - t_0 t_1 z \rangle \subset \mathbb{C}[t_0, t_1, x, y, z].$$

Using Example 4.3.8, the elimination ideal of J is

$$\hat{J} = (J : \langle t_0, t_1 \rangle^\infty) \cap K[x, y, z] = \langle y^2 - xz \rangle \subset K[x, y, z].$$

Then the morphism Φ is a parametrization of the parabola in $\mathbb{P}^2_{\mathbb{C}}$.

4.4.5 Example. The Veronese surface $S \subset \mathbb{P}^5_{\mathbb{C}}$ is defined as the image of the morphism

$$\begin{array}{rccc} \Phi : & \mathbb{P}^2_{\mathbb{C}} & \longrightarrow & \mathbb{P}^5_{\mathbb{C}} \\ & (t_0 : t_1 : t_2) & \longmapsto & (t_0^2 : t_1^2 : t_2^2 : 2t_0 t_1 : 2t_0 t_2 : 2t_1 t_2). \end{array}$$

Set

$$J = \left\langle \text{minors}_2 \begin{pmatrix} x_0 & x_1 & x_2 & x_3 & x_4 & x_5 \\ t_0^2 & t_1^2 & t_2^2 & 2t_0t_1 & 2t_0t_2 & 2t_1t_2 \end{pmatrix} \right\rangle \subset K[t_0, t_1, t_2, x_0, \ldots, x_5].$$

Using Singular, the elimination ideal of J is

$$\hat{J} = (J : \langle t_0, t_1, t_2 \rangle^\infty) \cap K[x_0, \ldots, x_5] = \left\langle \begin{array}{c} x_3x_4 - 2x_0x_5, 2x_1x_4 - x_3x_5, 2x_2x_3 - x_4x_5, \\ 4x_1x_2 - x_5^2, 4x_0x_2 - x_4^2, 4x_0x_1 - x_3^2 \end{array} \right\rangle \subset K[x_0, \ldots, x_5].$$

It follows that the Veronese surface is defined by

$$S = V(\hat{J}) \subset \mathbb{P}^5_{\mathbb{C}}.$$

Now, we consider the general case of rational map between projective algebraic varieties.

4.4.6 Definition. A rational map between projective varieties is a map

$$\Phi = (\overline{f_0} : \ldots : \overline{f_n}) : X = V(I) \subset \mathbb{P}^m_K \dashrightarrow \mathbb{P}^n_K,\ t \mapsto (\overline{f_0}(t) : \ldots : \overline{f_n}(t))$$

where $I \subset K[t_0, \ldots, t_m]$ is a homogeneous ideal, $\overline{f_i} \in K[t_0, \ldots, t_m]/I$ are homogeneous of the same degree, $\overline{f_i}(t) := f_i(t)$.
The domain of definition of the rational map Φ is

$$D(\Phi) = X \setminus \bigcap \left\{ V(I + \langle g_0, \ldots, g_n \rangle) \,|\, g_i \in K[t_0, \ldots, t_m],\ \text{minors}_2 \begin{pmatrix} g_0 & \cdots & g_n \\ f_0 & \cdots & f_n \end{pmatrix} = 0 \right\}.$$

The image of the rational map Φ is definied by

$$\text{im}(\Phi) = \Phi(D(\Phi)).$$

A rational map $\varphi : X \dashrightarrow Y$ is called a birational map if it has a rational inverse $\varphi^{-1} : Y \dashrightarrow X.q$

4.4.7 Remark. In Definition 4.4.6 the ring $K[t_0, \ldots, t_m]/I$ inherits a grading from the polynomial ring $K[t_0, \ldots, t_m]$ because the ideal I is homogeneous. The map Φ is well defined since for $t \in V(I)$, the definition

$$\overline{f_i}(t) := f_i(t)$$

is independent of the representative of the class f_i.

4.4.8 Theorem. *(Boehm, 2017) Let K an algebraically closed fields, $I \subset K[t_0, \ldots, t_m]$ a homogeneous ideal and*

$$\begin{array}{rccc} \Phi : & X = V(I) \subset \mathbb{P}^m_K & \dashrightarrow & \mathbb{P}^n_K \\ & t = (t_0 : \ldots : t_m) & \longmapsto & (\overline{f_0}(t) : \ldots : \overline{f_n}(t)) \end{array}$$

a rational map with $\overline{f_i} \in K[t_1, \ldots, t_m]/I$ homogeneous of the same degree. Then

$$\overline{im(\Phi)} = V((J : \langle f_0, \ldots, f_n \rangle^\infty) \cap K[x_0, \ldots, x_n])$$

where

$$J = \left\langle I, minors_2 \begin{pmatrix} x_0 & \cdots & x_n \\ f_0 & \cdots & f_n \end{pmatrix} \right\rangle \subset K[t_0, \ldots, t_m, x_0, \ldots, x_n].$$

Moreover, if the domain of definition $D(\Phi) = X$, then the image $im(\Phi)$ is Zariski closed.

Proof. A similar argument in the proof of Corollary 4.3.6 proves that the ideal $J : \langle f_0, \dots, f_n \rangle^\infty$ is bihomogeneous. Then we can define the vanishing locus

$$V(J : \langle f_0, \dots, f_n \rangle^\infty) \subset \mathbb{P}^m_K \times \mathbb{P}^n_K$$

and the graph of the map Φ is

$$\Gamma(\Phi) = V(J : \langle f_0, \dots, f_n \rangle^\infty) \subset \mathbb{P}^m_K \times \mathbb{P}^n_K.$$

From a topological point of view, Theorem 4.3.5 means that the projection π onto the second component $\mathbb{P}^n_K$ is a closed map. Moreover, it is also continuous. From topology, see for example (Bourbaki, 1995, Chapter 5, Proposition 9), gives

$$\begin{aligned}
\overline{\pi(\Gamma(\Phi))} &= \pi(\overline{\Gamma(\Phi)}) \\
\overline{\mathrm{im}(\Phi)} &= \pi(\overline{V(J : \langle f_0, \dots, f_n \rangle^\infty)}) \\
&= \pi(V(J : \langle f_0, \dots, f_n \rangle^\infty)) \\
&= V(((J : \langle f_0, \dots, f_n \rangle^\infty) : \langle t_0, \dots, t_n \rangle^\infty) \cap K[x_0, \dots, x_n]) \quad \text{by Theorem 4.3.5} \\
&= V((J : \langle f_0, \dots, f_n \rangle^\infty) \cap K[x_0, \dots, x_n])
\end{aligned}$$

If the rational map Φ is a morphism, the graph of Φ will be

$$\Gamma(\Phi) = V(J) \subset V(I) \times \mathbb{P}^n_K \subset \mathbb{P}^m_K \times \mathbb{P}^n_K.$$

The restriction of the projection map π to $V(I) \times \mathbb{P}^n_K$ and the same argument in proof of Theorem 4.3.5 imply

$$\mathrm{im}(\Phi) = V((J : \langle t_0, \dots, t_m \rangle^\infty) \cap K[x_0, \dots, x_n]) \subset \mathbb{P}^n_K.$$

□

4.4.9 Example. Consider $I = \langle t_0^2 - t_1^2 - t_2^2 \rangle \subset \mathbb{C}[t_0, t_1, t_2]$ ideal and the rational map

$$\begin{array}{rccc} \Phi : & V(I) \subset \mathbb{P}^2_{\mathbb{C}} & \dashrightarrow & \mathbb{P}^1_{\mathbb{C}} \\ & (t_0 : t_1 : t_2) & \longmapsto & (\overline{t_0 + t_1} : \overline{t_2}) \end{array}$$

Set

$$J = \left\langle I, \mathrm{minors}_2 \begin{pmatrix} x_0 & x_1 \\ t_0 + t_1 & t_2 \end{pmatrix} \right\rangle = \langle t_0^2 - t_1^2 - t_2^2, t_2 x_0 - t_0 x_1 - t_1 x_1 \rangle \subset K[t_0, t_1, t_2, x_0, x_1].$$

Using the command `sat` in Singular, we get

$$J : \langle t_0, t_1, t_2 \rangle^\infty = \langle t_2 x_0 - t_0 x_1 - t_1 x_1, t_0^2 - t_1^2 - t_2^2 \rangle$$

using as ordering the degree reverse lexicographical ordering `dp`.
Thus

$$(J : \langle t_0, t_1, t_2 \rangle^\infty) \cap K[x_0, x_1] = \langle 0 \rangle \subset K[x_0, x_1].$$

As $\Phi((1, -1, 0))$ is not defined, the rational map Φ is not a morphism. By Theorem 4.4.8, it follows that

$$\overline{\mathrm{im}(\Phi)} = V(\langle 0 \rangle) = \mathbb{P}^1_{\mathbb{C}}.$$

4.4.10 Algorithm. The procedure `ImageMap` in (Bitbucket, modimage.lib) computes the closure of the image of rational map seen in Theorem 4.4.8. It returns a ring containing an ideal called `image` defining the closure of the image.

5. Modular algorithm for the image of a rational map

An alternative method for computing in commutative algebra is the modular methods. In this chapter, a modular version of computing projective elimination will be presented. First, we will start with a general setting for computing saturations. Then we will extend to an algorithm for computing the closure of image of rational maps.

5.1 Modular algorithm for saturation

A Modular algorithm for computing saturations of ideals needs settings discussed in Chapter 3.

5.1.1 Setup.
Let $I, J \subset K[t_1, \ldots, t_m]$ be ideals and $>$ a global ordering on the set of monomials in the variables $t_1, \ldots, t_m$.
The ideal I is related to the ideal $U(0) = I : J^\infty \subset K[t_1, \ldots, t_m]$. For a prime number p, the reduction modulo p ideal $I_p \subset (\mathbb{Z}/p\mathbb{Z})[t_1, \ldots, t_m]$ of I is related to the ideal $U(p) = I_p : J_p^\infty \subset (\mathbb{Z}/p\mathbb{Z})[t_1, \ldots, t_m]$. To compute $U(p)$ from I_p, we will use the iteration of ideal quotients in Algorithm 4.2.9 (ii). In Singular, it corresponds to the command `sat`$(\cdot, \cdot)$ which returns a Gröbner basis of $I_p : J_p^\infty$ and the smallest integer $N \geq 2$ such that $I_p : J_p^\infty = I_p : J_p^N$. The general assumption is also satisfied.

5.1.2 Lemma. For all but finitely many primes $p \in \mathbb{N}$, we have $U(0)_p = U(p)$.

Proof. Let $N \geq 0$ be the integer such that $I : J^\infty = I : J^N$. If the prime p does not divide any numerator and denominator of any coefficient of any polynomial occurring when computing $I : J^{N+1}$, from $I : J^N = I : J^{N+1}$ we get $I_p : J_p^N = I_p : J_p^{N+1}$. This means that $I_p : J_p^\infty = I_p : J_p^N$. □

Furthermore, we can add the smallest integer $N_p \geq 0$ with $I_p : J_p^\infty = I_p : J_p^{N_p}$ to the majority vote and get a way of verification of the correctness. Indeed, we define the equivalence relation $\sim$ on the set of primes $\mathcal{P}$ used by

$$p \sim q \Longleftrightarrow \mathrm{LM}(U(p)) = \mathrm{LM}(U(q)) \text{ and } N_p = N_q.$$

The majority vote will replace $\mathcal{P}$ by an equivalence class of largest cardinality. If p is in this class $N_p = N$ is independent of p. The integer N is likely an integer satisfying

$$I : J^N = I : J^{N+1} \text{ and } U = I : J^N.$$

This means that $I : J^\infty = U$ by Proposition 4.2.2. As $I : J^N \subset I : J^{N+1}$, it remains to check if

$$U = I : J^N \text{ and } U : J \subset U.$$

5.1.3 Algorithm.

Algorithm Modular algorithm for computing saturation

Input: Ideal $I, J \subset K[t_1, \ldots, t_m]$.
Output: The ideal $U(0) = I : J$ and integer $N \geq 0$ such that $I : J^N = I : J^\infty$.

1: Choose a finite set of random primes $\mathcal{P}$.
2: Compute $U(p)$ for all $p \in \mathcal{P}$ and $N_p \in \mathbb{N}$ such that $U(p) = I_p : J_p^\infty = I_p : J_p^{N_p}$.
3: Delete primes in $\mathcal{P}$ respecting to a majority vote on $(\mathrm{LM}(U(p)), N_p)$ and set $N = N_p$.
4: Use Chinese remainder theorem to lift the result to $U(M)$ where $M = \prod_{p\in\mathcal{P}} p$.
5: Reconstruct $U(M)$ via error tolerant reconstruction and get U.
6: **if** $U_p = U(p)$ for a random prime $p \notin \mathcal{P}$ **then**
7: **return** U and N.
8: **else**
9: Enlarge $\mathcal{P}$ and repeat from 2.
10: **end if**
11: **return** U and N.

See (Bitbucket, modimage.lib) for the implementation on Singular via the procedure `modsat` and `pTest_sat`.

5.1.4 Verification.

Let $N \geq 0$ and integer, the ideal $I : J^N \subset K[t_1, \ldots, t_m]$ is equal to $I : J^\infty$ if and only if $I : J^N = I : J^{N+1}$. This follows from the proof of Proposition 4.2.2 (i).

5.1.5 Algorithm.

Algorithm Verification of saturations

Input: Ideals $I, J, U \subset K[t_1, \ldots, t_m]$, integer $N \geq 1$.
Output: `True` if U is the saturation of I by J else `False`.

1: **if** $U = I : J^N$ and $U : J \subset U$ **then**
2: **return** `True`.
3: **else**
4: **return** `False`.
5: **end if**

The procedures `finalTest_sat` in (Bitbucket, modimage.lib) implement this algorithm.

5.1.6 Example. Let $I = \langle x^2(y-1)\rangle, J = \langle x\rangle \subset \mathbb{Q}[x, y]$ and $\mathcal{P} = \{2, 3\}$, take the degree reverse lexicographical ordering `dp` as global ordering. Using the command `sat` in Singular, we have

$$U(2) = I_2 : J_2^\infty = \langle y + 1\rangle \subset (\mathbb{Z}/2\mathbb{Z})[x, y] \text{ and } N_2 = 2,$$
$$U(3) = I_3 : J_3^\infty = \langle y - 1\rangle \subset (\mathbb{Z}/3\mathbb{Z})[x, y] \text{ and } N_3 = 2.$$

The majority vote respecting $(\mathrm{LM}(U(p)), N_p)$ yields the set $\mathcal{P} = \{2, 3\}$ and $N = 2$. Then the Chinese remainder lifts $U(2)$ and $U(3)$ to

$$U(6) = \langle y - 1\rangle \subset (\mathbb{Z}/6\mathbb{Z})[x, y].$$

The procedure `ErrorTolerantReconstraction` appllied to $U(6)$ reconstructs

$$U = \langle y - 1 \rangle \subset Q[x, y].$$

Let take $p = 5$. We have $U(p) = \langle y - 1 \rangle \subset (\mathbb{Z}/5\mathbb{Z})[x, y]$ which matches with the ideal U_p. For the final test, we have

$$I : J^2 = \langle y - 1 \rangle \text{ and } I : J^3 = \langle y - 1 \rangle.$$

The test is a success. Then the algorithm returns the right ideal

$$I : J^\infty = \langle y - 1 \rangle \subset \mathbb{Q}[x, y].$$

5.2 Modular algorithm for computing the image of rational map

Algorithm 4.4.8 induces an algorithm computing the image of rational map of projective spaces.

5.2.1 Setup.

Fix a global ordering on $K[t_0, \ldots, t_m, x_0, \ldots, x_n]$ which is an elimination ordering for the variables $t_0, \ldots, t_m$.

Let

$$\begin{array}{rccc} \Phi : & V(I) \subset \mathbb{P}^m_K & \longrightarrow & \mathbb{P}^n_K \\ & t = (t_0 : \cdots : t_m) & \longmapsto & (f_0(t) : \cdots : f_n(t)) \end{array}$$

a rational map with $f_i \in K[t_1, \ldots, t_m]$ homogeneous and have the same degree, $I \subset K[t_0, \ldots, t_m]$ a homogeneous ideal. Set

$$J = \left\langle I, \text{minors}_2 \begin{pmatrix} x_0 & \cdots & x_n \\ f_0 & \cdots & f_n \end{pmatrix} \right\rangle \subset K[t_0, \ldots, t_m, x_0, \ldots, x_n].$$

By Theorem 4.4.8, the ideal $U(0) = (J : \langle f_0, \ldots, f_n \rangle^\infty) \cap K[x_0, \ldots, x_n]$ gives the closure of the image of the rational map Φ by $V(\hat{J}) \subset \mathbb{P}^n_K$.

5.2.2 Algorithm.

Algorithm Modular algorithm for computing image of rational map

Input: Rational map Φ defined by polynomials $f_0, \ldots, f_n \in \mathbb{Q}[t_1, \ldots, t_m]$, ideal $I \subset \mathbb{Q}[t_0, \ldots, t_n]$

Output: The ideal of the closure of image $\hat{J}$.

1: Compute the ideal

$$J = \left\langle I, \text{minors}_2 \begin{pmatrix} x_0 & \cdots & x_n \\ f_0 & \cdots & f_n \end{pmatrix} \right\rangle \subset \mathbb{Q}[t_0, \ldots, t_m, x_0, \ldots, x_n].$$

2: Choose a finite set of random primes $\mathcal{P}$.
3: Compute $U(p) = (J_p : \langle f_0, \ldots, f_n \rangle_p^\infty) \cap (\mathbb{Z}/p\mathbb{Z})[x_0, \ldots, x_n]$ for all $p \in \mathcal{P}$.
4: Delete primes in $\mathcal{P}$ respecting to a majority vote on LM$(U(p))$.
5: Use Chinese remainder theorem to lift the result to $U(N)$ where $N = \prod_{p \in \mathcal{P}} p$.
6: Reconstruct $U(N)$ via error tolerant reconstruction and get U.
7: **if** $U_p = U(p)$ for a random prime $p \notin \mathcal{P}$ **then**
8: **return** U.
9: **else**
10: Enlarge $\mathcal{P}$ and repeat from 3.
11: **end if**

See the procedure `ModImageMap` in (Bitbucket, modimage.lib) for the implementation using Singular. The parallel version of Algorithm 5.2.2 is also implemented in Singular via the procedure `ModImageMapPar` in (Bitbucket, modimage.lib).

5.2.3 Example. Consider the morphism

$$\begin{array}{rccc} \Phi: & \mathbb{P}^1_{\mathbb{Q}} & \longrightarrow & \mathbb{P}^3_{\mathbb{Q}} \\ & (t_0 : t_1) & \longmapsto & (t_0^2 : t_0t_1 : t_1^2). \end{array}$$

Set

$$J = \left\langle \text{minors}_2 \begin{pmatrix} x & y & z \\ t_0^2 & t_0t_1 & t_1^2 \end{pmatrix} \right\rangle = \langle t_0t_1x - yt_0^2, t_1^2x - t_0^2z, t_1^2y - t_0t_1z\rangle \subset \mathbb{Q}[t_0, t_1, x, y, z].$$

Choose $\mathcal{P} = \{2, 3\}$. Singular gives

$$\begin{aligned} U(2) &= J : \langle t_0, t_1\rangle^\infty = \langle y^2 + xz, t_0z + t_1y, t_0y + t_1x\rangle \subset (\mathbb{Z}/2\mathbb{Z})[t_0, t_1, x, y, z], \\ U(3) &= J : \langle t_0, t_1\rangle^\infty = \langle y^2 - xz, t_0z - t_1y, t_0y - t_1x\rangle \subset (\mathbb{Z}/3\mathbb{Z})[t_0, t_1, x, y, z]. \end{aligned}$$

It follows that $\mathcal{P} = \{2, 3\}$ after the majority vote. The Chinese remainder lifts the modular results $U(2)$ and $U(3)$ to

$$U(6) = \langle y^2 - xz, t_0z - t_1y, t_0y - t_1x\rangle \subset (\mathbb{Z}/6\mathbb{Z})[t_0, t_1, x, y, z].$$

Then, the error tolerant reconstruction lifts $U(6)$ to

$$U = \langle y^2 - xz, t_0z - t_1y, t_0y - t_1x\rangle \subset \mathbb{Q}[t_0, t_1, x, y, z].$$

Since $G = \{y^2 - xz, t_0z - t_1y, t_0y - t_1x\}$ is a Gröbner basis of U, we have

$$G \cap K[x, y, z] = \{y^2 - xz\}$$

and the algorithm returns the ideal

$$J = \langle y^2 - xy\rangle \subset K[x, y, z].$$

This is the true answer as we have seen in Example 4.4.4.

6. Timings and conclusion

6.1 Timings

In this section, we provide examples on which we time Algorithm 4.4.10 and Algorithm 5.2.2. We have implemented them using the programming language Singular. Timings are conducted by using the version of Singular $4.1.2$ on an Intel(R) core (TM) $\mathrm{i}5-8500$ CPU @ 3.00 Ghz (6 cores), 16 GB RAM DDR4 Synchronous 2666Mhz under a linux operating system (AIMS desktop).
Examples are chosen to emphasize the performance of the modular method. The results are summarized in the Table 6.1.

6.1.1 Example.

$$\begin{aligned} I =&\langle t_1^5 + 10t_1^4t_2 + 20t_1^3t_2^2 + 130t_1^2t_2^3 - 20t_1t_2^4 + 20t_2^5 - 2t_1^4t0 - 40t_1^3t_2t_0 - 150t_1^2t_2^2t_0 - 90t_1t_2^3t_0 - \\ & 40t_2^4t_0 + t_1^3t_0^2 + 30t_1^2t_2t_0^2 + 110t_1t_2^2t_0^2 + 20t_2^3t_0^2\rangle \subset \mathbb{Q}[t_0, t_1, t_2], \\ \Phi =&(t_2^3 : t_1t_2^2 : t_1^2t_2 : t_1^3 : t_0t_2^2 : t_0t_1t_2 : t_0t_1^2 : t_0^2t_2 : t_0^2t_1 : t_0^3). \end{aligned}$$

In the next examples, we take the same ideal I as in Example 6.1.1 but different rational maps Φ.

6.1.2 Example. See (Bitbucket, example.sing).

6.1.3 Example. See (Bitbucket, example.sing).

6.1.4 Example. See (Bitbucket, example.sing).

6.1.5 Example. See (Bitbucket, example.sing).

6.1.6 Example. See (Bitbucket, example.sing).

Example	Degree of Φ	`ImageMap`	`ModImageMap`	`ModImageMapPar[2]`	`ModImageMapPar[6]`
6.1.1	3	137	1618	1050	680
6.1.2	8	1783	159	101	56
6.1.3	15	58980	581	348	183
6.1.4	20	315258	1157	3205	381
6.1.5	22	545339	1474	843	439
6.1.6	25	1313034	2124	1237	674

Table 6.1: Running times in millisecond for `ImageMap`, `ModImageMap` and `ModImageMapPar`. The notation `ModImageMapPar[n]` means running the parallel algorithm `ModImageMapPar` using exactly n cores of the computer.

6.2 Conclusion

Theses timings show that the modular algorithm computing the image of a rational map has a good performance in examples with large coefficients. It is much faster than the direct approach. Nevertheless, the algorithms is probabilistic. Regardless, future research could continue to explore a modular algorithm computing the image of a birational map in which we may think of a way of verification of the result.

Acknowledgements

Foremost, praises and thanks to God, the Almighty, for this showers of blessings throughout my research work.

Next, I would like to express my sincere gratitude to my advisor Dr. Magdaleen Marais, Dr. Janko Böhm and Dr. Dirk Basson for their patience, guidance, help, and immense knowledge to make this work possible.

I want to acknowledge AIMS in particular Prof. Barry Green the Director of AIMS South Africa and Dr. Simukai Utete the Academic Director of AIMS South Africa and my tutor Dr. Prudence Djagba.

Last but not least, I give thanks to my family for their prayers, caring, and sacrifices.

References

A. Altman and S. Kleiman. *A Term of Commutative Algebra*. Worldwide Center of Mathematics, 2013.

E. A. Arnold. Modular algorithms for computing Gröbner bases. *Journal of Symbolic Computation*, 35: 403–419, 2003.

M. F. Atiyah and I. G. Macdonald. *Introduction to Commutative algebra*. Addison-Wesley publishing company, 1969.

Bitbucket. Singular code. https://bitbucket.org/hobihasina/singular-code/src/master/.

J. Boehm. *Computer Algebra*. Lecture notes, Univeristy of Kaiserslautern, 2017.

J. Boehm, W. Decker, C. Fieker, and G. Pfister. The use of bad primes in rational reconstruction. *Math. Comp.*, 84, 2015.

J. Boehm, W. Decker, C. Fieker, S. Laplagne, and G. Pfister. Bad primes in computational algebraic geometry. *arxiv:1702.06920*, 2017.

N. Bourbaki. *General Topology*. Springer, 1995.

M. R. Bremner. *Lattice Basis reduction*. Taylor and Francis Group, 2012.

D. A. Cox, J. Little, and D. O'Shea. *Ideals, Varieties and Algorithms : An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer, 2015.

W. Decker and G. Pfister. *A First Course in Computational Algebraic Geometry*. Cambridge University Press, 2011.

W. Decker, G.-M. Greuel, G. Pfister, and H. Schönemann. Singular 4-1-2 — A computer algebra system for polynomial computations. https://www.singular.uni-kl.de/, accessed May 2020.

D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*. Springer, 1995.

J. A. Gallian. *Contemporary Abstract Algebra*. Brooks/Cole, 2012.

G.-M. Greuel and G. Pfister. *A Singular Introduction to Commutative algebra*. Springer, 2008.

G. Kemper. *A Course in Commutative Algebra*. Springer, 2010.

P. Kornerup and R. T. Gregory. Mapping intergers and hensel codes onto farey fractions. *BIT*, 23:9–20, 1983.

H. M. Moeller and F. Mora. Degree upper and lower bounds for the degree of Gröbner bases. *Eurosam'84, Lecture Notes in Computer Science*, 174:172–183, 1984.

paraplanecurves.lib. Singular library. https://github.com/Singular/Sources/blob/spielwiese/Singular/LIB/paraplanecurves.lib, accessed May 2020.