Polynomial factorization and curve decomposition algorithms

Cristina Bertone

UNIVERSITÁ DEGLI STUDI DI TORINO
FACOLTÁ DI SCIENZE MATEMATICHE FISICHE E NATURALI

UNIVERSITÉ DE NICE SOPHIA ANTIPOLIS
FACULTÉ DES SCIENCES DE NICE

THÈSE DE DOCTORAT

pour l'obtention du titre de

Dottore in Scienza e Alta Tecnologia, indirizzo Matematica

Docteur en Sciences, specialité Mathématiques

présentée par

Cristina Bertone

Polynomial factorization and curve decomposition algorithms

Soutenue le 26 mars 2010 devant le jury composé de :

M.	Alberto Conte,	Examinateur
M.	André Galligo,	Directeur
M.	Grègoire Lecerf,	Examinateur
M.	Bernard Mourrain,	Examinateur
Mme.	Margherita Roggero,	Directeur
M.	Carlo Traverso,	Rapporteur

Introduction

Consider a set of polynomials $\{F_1, \ldots, F_s\} \subseteq \mathbb{K}[X_1, \ldots, X_n]$, $\mathbb{K}$ a field, and consider its *set of zeros*

$$V(F_1, \ldots, F_s) = \{P \in \overline{\mathbb{K}}^n | F_i(P) = 0, i = 1, \ldots, s\}.$$

The set of points $V(F_1, \ldots, F_s)$ is an *algebraic set* or a *variety* of $\overline{\mathbb{K}}^n$, $\overline{\mathbb{K}}$ the algebraic closure of $\mathbb{K}$. Actually, this set of points is the same as $V(\mathfrak{a})$, where $\mathfrak{a}$ is the ideal in $\mathbb{K}[X_1, \ldots, X_n]$ generated by the set of polynomials $\{F_1, \ldots, F_s\}$. An algebraic set is said to be *irreducible* if it can not be expressed as the union of two proper algebraic subsets, and it is said to be *reducible* otherwise. If we consider a reducible algebraic set and we write it as union of irreducible algebraic subsets, these are the *irreducible components* (or simply the *components*).

We will consider an algebraic curve (that is, an algebraic set of dimension 1) in the affine space $\mathbb{C}^2$ or $\mathbb{C}^3$ and our aim is to find its irreducible components, i.e. the polynomials defining them.
In both affine spaces, the decomposition of a curve exists and is unique, in the sense that there is a finite number of irreducible components which are uniquely determined. We are interested in developing a practical method to construct this decomposition.

In mathematics, we often deal with geometric problems in higher dimensional spaces by means of induction: that is, once the problem is solved in a "smaller" space, you can solve the problem also in a "bigger" space through the known properties of the small one.
This is what we plan to do, we will bring back the problem of decomposing a curve in $\mathbb{C}^3$ to the problem of decomposing a curve in $\mathbb{C}^2$.

Nevertheless, at a first sight, the situation in $\mathbb{C}^3$ is dramatically different from the situation in $\mathbb{C}^2$.

$\mathbb{C}^2$: a curve $\mathscr{C}$ is an algebraic set of dimension 1, so it is defined by a principal ideal:

$$V(\mathfrak{a}) = \mathscr{C} \quad \text{with } \mathfrak{a} = (f(X, Y)) \subseteq \mathbb{C}[X, Y].$$

Then, $\mathscr{C}$ is irreducible if and only if $f(X, Y)$ is irreducible in $\mathbb{C}[X, Y]$. The problem of decomposing $\mathscr{C}$ in its irreducible components $\mathscr{C}_1, \ldots, \mathscr{C}_s$ is then equivalent to the problem of computing the factorization of $f(X, Y)$ in $\mathbb{C}[X, Y]$.

$\mathbb{C}^3$: a curve $\mathscr{C}$ is not defined by a single polynomial, we need 2 (or more). In this case, the decomposition of $\mathscr{C}$ in $\mathscr{C}_1, \ldots, \mathscr{C}_s$ is equivalent to the primary decomposition of the ideal $\mathfrak{a}$, such that $V(\mathfrak{a}) = \mathscr{C}$.

In the thesis we will study the decomposition of curves defined by rational polynomials.

The problem of absolute factorization (and rational factorization) was studied by many authors, who proposed more and more performing algorithms (see [45], [46] for a survey on the history of the subject).
On the contrary, the problem of computing the primary decomposition of an ideal $\mathfrak{a}$ of $\mathbb{C}[X_1, \ldots, X_n]$ was tackled with different techniques (see for instance [21] and the references therein) and the research in this field is in continuous progress (for example, the case of 0-dimensional ideals, see [23]). However, there is not yet an efficient strategy for the general case. Two of the most recent strategies for curves in $\mathbb{C}^3$ rely on the reduction to the case of a set of points on a plane and use numerical computations (see [29], [73]).
In fact, it is computationally advantageous to solve the problem passing from an algebraic set of dimension 1 in $\mathbb{C}^3$ to an algebraic set of dimension 0 in $\mathbb{C}^2$. Indeed passing from a curve in $\mathbb{C}^3$ to a curve in $\mathbb{C}^2$ would require hard computations.

Nevertheless, this is exactly what we will do: once studied an absolute factorization algorithm for bivariate polynomials, we will try to use the same techniques for a curve in $\mathbb{C}^3$ by projection on a generic plane; the technique of generic projection and absolute factorization is "classical", but we will be able to speed up computations since our techniques are modular.

In Chapter 1, we study the problem for $n = 2$, so we deal with the computation of the absolute factorization of a rational polynomial. This problem was extensively studied in the recent years (see [15], [68], [72], [16] and the references therein), but we focus here on Trager-Traverso Algorithm (see [24], [44], [78] and Section 1.2 with Algorithm 1). On the one hand the idea is to follow the same strategy, on the other one to improve it: we will exploit modular computations in order to obtain faster and better results. Indeed using this tool, we are able to describe an absolute irreducibility test (Algorithm 2) and then develop modular techniques (Section 1.4) in order to have an absolute factorization algorithm (Algorithm 4). Its main aim is the same as Trager-Traverso's one, but it gets sharper results (in the sense of the degree of the algebraic extension).
The absolute irreducibility test is based on some properties of the Newton polytope of the polynomial. The absolute factorization algorithm constructs an algebraic extension of $\mathbb{Q}$ which contains the coefficients of the absolute factors and has minimal degree. This is obtained through a careful choice of a prime integer p which ensures that we have a primitive element of the algebraic extension needed in $\mathbb{Q}_p$, the field of p-adic numbers (Lemma 1.4.9). Relying on randomness, we can say that generally this choice of p gives a good reduction of

$f(X,Y)$, i. e. the factorization of $f(X,Y)$ modulo p is a p-adic approximation of its absolute factorization. We then use Hensel lifting to obtain a more precise p-adic approximation of a primitive algebraic element and we finally construct a univariate polynomial defining the algebraic extension using the LLL algorithm.
In the appendix (Chapter A and B) we summarize the main definitions and properties concerning the LLL algorithm and the field of p-adic numbers.

In Chapter 2 we underline the main differences and similarities between the cases $n = 2$ and $n = 3$: to do this, we start with some basic definitions and properties about the primary decomposition of an ideal and the affine Hilbert function. We consider a complete intersection ideal $\mathfrak{a}$ and we define the rational, the algebraic and the conjugated components for a primary decomposition, in parallel with the absolute factorization of a polynomial. Using Hilbert function, we have also the definitions of degree and multiplicity of a primary component.
After this, we exactly state the output of our decomposition algorithm for a curve in $\mathbb{C}^3$, which is the same one of other existing algorithms ([29], [73]). For each irreducible algebraic component we would like to construct a separator polynomial (Definition 2.2.6): it is a polynomial defining an algebraic surface which contains a component but not the other ones. Furthermore, we point out the problem of having a bound on the degree of a separator polynomial; if we could have such a bound, we could use it inside a numerical algorithm of decomposition to avoid extra and unnecessary computations.

In Chapter 3 we focus on bounds on the degree of a separator polynomial using algebraic geometry invariants and arguments existing in literature. We look for such a bound in three different ways: through a plane section, a particular case of the classical Lifting Problem in codimension 2 (Section 3.2); through the regularity of the ideal (Section 3.3) and through the generic initial ideal (Section 3.4).
The Lifting Problem in codimension 2 is a classical one in algebraic geometry. Although the case of curves in the 3-dimensional space is completely solved, the problem is still open in higher dimensions. Laudal's generalized trisecant lemma and the following improvements (see [50], [76], [38]) give a lower bound on the degree of a separator polynomial, by computing the generic plane section. About the Lifting Problem, we also briefly resume some original results concerning the positivity of the second Chern Class of a reflexive sheaf (Section 3.2.1), which is one of the directions of investigation to prove Mezzetti's conjecture (Conjecture 3.2.1).
The regularity is a well-known invariant for ideals, which bounds not only the degrees of the minimal generators of the ideal, but also their syzygies. Using the regularity, we can bound the degree of a separator polynomial in several ways: with the degree of the component and in particular cases with the regularity of the plane section or with a linear function in the

degrees of the generators of the ideal $\mathfrak{a}$; we use results in [37], [58], [11], [17].
Finally, the generic initial ideal is a monomial ideal which has combinatorial features reflecting invariants of the ideal, such as its saturation or the regularity itself (see [35]). Then the generic initial ideal of a component immediately gives the desired bound on the degree of the separator polynomial.

Since any of the "classical" bounds in Chapter 3 is not actually practical or useful for our purposes, we expose in Chapter 4 an obvious strategy to find the primary decomposition of an ideal (or at least its primary components which are also prime). This strategy uses generic projections (which were first used in [41], but still effective, e.g [72]). Projections allow us to bring back the problem of decomposition of a 3-dimensional curve to the problem of factoring a bivariate polynomial. Then, by means of Hilbert dimension (to match couples of factors coming from two different projections) and of quotient ideals (to take off embedded points, which are actually in the singular locus of the ideal), we can get the ideals defining the prime components of $\mathfrak{a}$ (that is, primary components of multiplicity 1). This exact strategy is illustrated in Algorithms 7 and 6. Actually, a "generic projection" is obtained through a generic change of coordinates and a projection on a coordinate plane (in practice, the computation of a resultant).
Unfortunately, this strategy is not advantageous from the computational point of view, so we again use modular computations to make this strategy faster.
In Section 4.2 we show that we can rely on randomness (just like we do for absolute factorization) to avoid a bad prime p: in other words, if we just choose a prime p ensuring that an algebraic α is in $\mathbb{Q}_p$, then we are "almost" sure that an ideal $\mathfrak{a} \subseteq \mathbb{Q}(\alpha)[X_1, \ldots, X_n]$ can be reduced modulo p preserving its affine Hilbert function.
The results of Section 4.2 hold for ideals in a polynomial ring with n indeterminates, but we apply them to the irreducible components of a complete intersection ideal in $\mathbb{Q}[X, Y, Z]$: we adapt the algorithms of Section 4.1 to the modular computations; in particular, we by-pass the problems of computing the bivariate rational resultants and the bivariate absolute factorizations. Modular computations also speed up the computations of Hilbert dimensions and quotient ideals. As output of Algorithm 10 we obtain modular ideals whose Hilbert function are the same as the Hilbert functions of the prime components of $\mathfrak{a}$. These Hilbert functions obviously give us practical bounds on the degrees of the separator polynomials of each component.
In Section 4.3.2 we explicitly apply the modular strategy on an example: we further shorten the computations looking at the primality of the degrees of the factors in the modular factorization of resultants, using the consequences of Lemma 1.1.4. In this way we avoid to change the prime p if not necessary and we reduce the number of resultants and factorizations to compute.

Even if Algorithm 10 does not return the rational separator polynomials, but only their modular images, it is quite promising: indeed, we try to compute the primary decomposition of the ideal of Section 4.3.2 using the Maple routine conceived to do this, `PrimaryDecomposition`: it could not achieve the result on our example, nor on the rational or on the correct algebraic extension, because of problems in the memory allocation.

The practical bounds that we obtain can be used inside a numerical algorithm. In Section 4.4 we investigate how to use modular techniques in a different way on the decomposition algorithm presented in Section 4.1: we assume that we are able to compute the projection on a generic plane and a bivariate absolute factorization (by means of a rational factorization algorithm and an absolute one, such as Algorithm 4). After matching the couples of factors, for the prime components we can compute the quotient ideal with respect to an equation of the singular locus via modular Groebner Basis. We adapt the techniques described in [1] to the computation of a quotient ideal with respect to a principal ideal in Algorithm 11.
Finally, we remark that in order to conclude Algorithm 10 with the lifting of the modular separator polynomials, we would need a generalization of Hensel lifting for rational ideals. The problem is quite easy to state (see Section 4.4.2) and we have some hints to solve it coming from the knowledge of Groebner Basis along the computations: assuming that we have a "good prime" p, we know that the possible monomials appearing with non-zero coefficient in a separator polynomial are in a known finite set. Nevertheless this conditions seem not be sufficient to lift the modular separator polynomials: we failed to lift the separator polynomials in the easy situation of a complete intersection ideal with purely rational components (Example 4.4.1).

In the conclusions, we summarize the achieved results, the possible improvements of the algorithms we have designed and how we could generalize them to higher dimensional problems.

Contents

List of Algorithms

Chapter 1

Absolute factorization of a rationally irreducible polynomial

This chapter is an extended version of [5].

1.1 Absolute Factorization

Assume that the curve $\mathscr{C}$ we wish to decompose is reduced and rationally irreducible, that is: the defining polynomial $f(X,Y)$ is not reducible over $\mathbb{Q}[X,Y]$.

We now recall the basic definitions and properties of the absolute factorization of a bivariate polynomial, following the approach of [15].

Definition 1.1.1. *Let A be a domain. We say that A is a* unique factorization domain *(UFD for short) if for all $a \in A \setminus \{0\}$ we can write $a = u \cdot p_1 \cdots p_s$ where u is a unit, $p_1, \ldots, p_s$ are irreducible in A and this decomposition is unique up to reordering and multiplication by units.*

If A is a UFD, then $A[X]$ is a UFD.

If k is a field, then $k[X_1, \ldots, X_n]$ is a UFD: for all $f \in k[X_1, \ldots, X_n]$, there exists $f = f_1 \cdots f_s$ (factorization), with f_i irreducible in $k[X_1, \ldots, X_n]$ and this decomposition is unique up to reordering and multiplication by constant factors.

Definition 1.1.2. *Let $K = \overline{k}$ be the algebraic closure of the field k, and $f \in k[X_1, \ldots, X_n]$. The factorization of f in $K[X_1, \ldots, X_n]$ is called the* absolute factorization *of f.*

Just to fix this idea, we can consider a very simple example.

Example 1.1.3. *Consider the bivariate polynomial $f = X^2 - 3Y^2$. f is irreducible in $\mathbb{Q}[X,Y]$ but it is reducible in $\overline{\mathbb{Q}}[X,Y]$:*

$$X^2 - 3Y^2 = (X - \sqrt{3}Y)(X + \sqrt{3}Y) \in \overline{\mathbb{Q}}[X,Y].$$

Actually, in this case, we do not need the whole algebraic closure of the field of rational numbers: the coefficients of the absolute factors are in the simple algebraic extension $\mathbb{Q}(\sqrt{3})$.

It is interesting to point out from Example 1.1.3, that the two factors of f have the same monomials and their coefficients are conjugate over $\mathbb{Q}$.
The next lemma generalizes this remark.

Lemma 1.1.4 (Fundamental Lemma)**.** *Let* $\mathbb{K}$ *be a perfect field and* $\overline{\mathbb{K}}$ *be its algebraic closure. Let* $f \in \mathbb{K}[X,Y]$ *be a monic and irreducible polynomial in* $\mathbb{K}[X,Y]$.

$$f(X,Y) = Y^n + a_{n-1}(X)Y^{n-1} + \cdots + a_0(X) \quad \textit{with } \deg(a_i(X)) \leq n-i.$$

Let $f = f_1 \cdots f_s$ *be the factorization of* f *into irreducible polynomials* $f_i \in \overline{\mathbb{K}}[X,Y]$. *Denote by* $\mathbb{L} = \mathbb{K}(\alpha)$ *the extension of* $\mathbb{K}$ *generated by all the coefficients of* f_1. *Then each* f_i *can be written as:*

$$f_i(X,Y) = Y^m + b_{m-1}(\alpha_i, X)Y^{m-1} + \cdots + b_0(\alpha_i, X), \tag{1.1.1}$$

with $b_k \in \mathbb{K}[Z,X]$, $\deg_X(b_k) \leq m-k$, *and where* $\alpha_1, \ldots, \alpha_s$ *are the different conjugates over* $\mathbb{K}$ *of* $\alpha = \alpha_1$.

Proof. We can suppose that each f_i is monic in Y , because f is monic in Y.

We set $f_i(X,Y) = Y^{n_i} + a^{(i)}_{n_i-1}(X)Y^{n_i-1} + \cdots + a^{(i)}_0(X)$ with $a^{(i)}_k(X) \in \overline{\mathbb{K}}[X]$ and $\deg_X(a^{(i)}_k(X)) \leq n_i - k$. Let $\mathbb{L}$ be the field generated by all the coefficients of f_1; since the field $\mathbb{K}$ is perfect, by the primitive element theorem we can set $\mathbb{L} = \mathbb{K}(\alpha)$; α is an algebraic number over $\mathbb{K}$ and we denote by $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_l$ its l different conjugates over $\mathbb{K}$, and by $\sigma_1, \ldots, \sigma_l$ the automorphism of $\mathbb{L}$ fixing $\mathbb{K}$ such that $\sigma_i(\alpha) = \alpha_i$.

Now we prove that $l \leq s$. Let $\mathbb{M}$ be the extension of $\mathbb{K}$ generated by the coefficients of $f_1, \ldots, f_s$; $\mathbb{M}$ is a finite extension of $\mathbb{K}$, and we have $\mathbb{C} \supseteq \mathbb{M} \supseteq \mathbb{L} \supseteq \mathbb{K}$. We can extend to $\mathbb{M}$ all the σ_i. Then we extend σ_i to $\mathbb{M}[X,Y]$, and we denote this map by $\tilde{\sigma}_i$. We have $\tilde{\sigma}_i(f) = \tilde{\sigma}_i(f_1) \cdots \tilde{\sigma}_i(f_s) = f$. Since $\mathbb{K}[X,Y]$ is a UFD, there exists an index j_0 such that $\tilde{\sigma}_i(f_1) = f_{j_0}$. Furthermore, if $\tilde{\sigma}_i(f_1) = \tilde{\sigma}_j(f_1)$ then $\tilde{\sigma}_i = \tilde{\sigma}_j$. So the map

$$\begin{aligned} ev_{f_1} : \{\tilde{\sigma}_1, ..., \tilde{\sigma}_k\} &\to \{f_1, ..., f_s\} \\ \tilde{\sigma}_i &\mapsto \tilde{\sigma}_i(f_1) \end{aligned}$$

is injective and $l \leq s$.

If $l < s$ we get an absurd result. Indeed, consider $F = \prod_{i=1}^{l} \tilde{\sigma}_i(f_1)$; this polynomial divides f so if we prove that $F \in \mathbb{K}[X,Y]$, we are done.
Write $f_1(X,Y) = \sum_{a,b} c_{a,b}(\alpha) X^a Y^b$ where $c_{i,j}(T) \in \mathbb{K}[T]$. Thus

$$F(X,Y) = \prod_{i=1}^{l} (\sum_{a,b} c_{i,j}(\alpha_i) X^a Y^b).$$

The coefficient of X^aY^b is written

$$\sum_{\substack{i_1+\cdots+i_k=a\\ j_1+\cdots+j_k=b}} c_{i_1,j_1}(\alpha_1)\cdots c_{i_k,j_k}(\alpha_k).$$

It is a symmetric polynomial in $\alpha_1,\cdots,\alpha_k$, so it is an element of $\mathbb{K}$; we deduce that $F(X,Y)\in\mathbb{K}[X,Y]$. □

Corollary 1.1.5. *Consider $f\in\mathbb{K}[X,Y]$ polynomial, irreducible in $\mathbb{K}[X,Y]$.*

- *the number of absolute factors s of f is equal to the degree extension $[\mathbb{L}:\mathbb{K}]$;*
- *$[\mathbb{L}:\mathbb{K}]$ divides $\operatorname{tdeg} f$;*
- *the absolute factorization of a bivariate polynomial is completely described by one absolute factor and a representation of the algebraic extension $\mathbb{L}$ of $\mathbb{K}$.*

Example 1.1.6. *We consider the absolute factorization*

$$f=X^2-3Y^2=(X-\sqrt{3}Y)(X+\sqrt{3}Y)\in\overline{\mathbb{Q}}[X,Y].$$

Assume that we just know $f_1=X-\sqrt{3}Y$.
We can observe that the field extension generated by f_1 is $\mathbb{Q}(\sqrt{3})$.
Furthermore, $[\mathbb{Q}(\sqrt{3}):\mathbb{Q}]=2$, which corresponds to the number of absolute factors, so we have two automorphism of $\mathbb{Q}(\sqrt{3})$ fixing $\mathbb{Q}$:

$$\sigma_1(\sqrt{3})=\sqrt{3}\qquad\sigma_2(\sqrt{3})=-\sqrt{3}.$$

If we apply σ_2 on f_1 we exactly obtain $f_2=X+\sqrt{3}Y$.

1.2 Trager-Traverso Algorithm

One can obtain the absolute factorization of a bivariate rational polynomial using one of the most popular programs in mathematics, Maple [54], using the command `AFactor`.

Example 1.2.1. *We can ask Maple to compute the absolute factorization of the polynomial f of Example 1.1.3.*

```
evala(AFactor(X^2-3*Y^2));
```

gives

```
(X-RootOf(Z^2-3)Y)(X+RootOf(Z^2-3)Y)
```

which exactly means $X^2 - 3Y^3 = (X - \alpha Y)(X + \alpha Y)$*, with* α *root of* $Z^2 - 3$*.*

Unfortunately, this Maple command is efficient for bivariate polynomials of degree≤ 15. Our challenge is to describe an algorithm having good performances on polynomials of much higher degree, 200 or more.

The algorithm implemented in Maple is Trager-Traverso Algorithm (or TKTD Algorithm, acronym for Trager-Kaltofen-Traverso-Dvornicich, see [24], [44], [78]), it consists of 4 steps.

Algorithm 1 Trager-Traverso algorithm

Input: $f(X, Y) \in \mathbb{Z}[X, Y]$ rationally irreducible.

Output: $f_1(X, Y)$ absolute factor of $f(X, Y)$.

1: Fix an integer value a of X such that $disc_Y f(a) \neq 0$.
2: Consider a root b of the polynomial $q(Y) = f(a, Y)$.
3: Compute a factorization of f in $\mathbb{Q}(b)[X, Y]$ and take $f_1(X, Y)$ as the factor such that $f_1(a, b) = 0$.
4: **return** The absolute factor $f_1(X, Y)$ of $f(X, Y)$.

Observe that the computation in Step 3 of Algorithm 1 does not provide a complete absolute factorization, but splits the polynomials into (at least) two factors in $\mathbb{L}[X, Y]$ with $\mathbb{L} = \mathbb{Q}[t]/q(t)$.

Remark 1.2.2. *We present a simplified version of Trager-Traverso algorithm: its complete form takes as input a multivariate polynomial which may be rationally reducible.*

Step 1 of Algorithm 1 relies on the following theorem.

Theorem 1.2.3 (Hilbert's irreducibility theorem)**.** *Let* $f(T_1, \ldots, T_r, X_1, \ldots, X_s)$ *be an irreducible polynomial in* $\mathbb{Q}[T_1, \ldots, T_r, X_1, \ldots, X_s]$*. Then almost all points* $(t_1, \ldots, t_r) \in \mathbb{Q}^r$ *are such that* $f(t_1, \ldots, t_r, X_1, \ldots, X_s)$ *is irreducible in* $\mathbb{Q}[X_1, \ldots, X_s]$*.*

In other words, Hilbert's irreducibility theorem states that if we specialize some of the variables of a rational polynomial with random values in $\mathbb{Q}$, then this specialization generally preserves the irreducible factors of the polynomial.

In Step 1 of Algorithm 1, we find a *simple* solution of f.

Definition 1.2.4. *Let* $\overline{\mathbb{K}}$ *be the algebraic closure of the field* $\mathbb{K}$*, and let* $(a, b) \in \overline{\mathbb{K}}^2$*. We say that* (a, b) *is a* simple solution *of* $f(X, Y) \in \mathbb{K}[X, Y]$ *when* $f(a, b) = 0$ *and either* $\frac{\partial f}{\partial X}(a, b)$ *or* $\frac{\partial f}{\partial Y}(a, b)$ *is non-zero.*

Theorem 1.2.5. *Let* (a, b) *be a simple solution of* $f(X, Y)$*. Then one absolute factor of* $f(X, Y)$ *belongs to* $\mathbb{K}(a, b)[X, Y]$*.*

The above theorem was demonstrated independently in [44] and [24].

In Step 3 of Algorithm 1, it is supposed that we have an algorithm of factorization on $\mathbb{K}(b)$. Supposing that we have this kind of algorithm for algebraic extensions of $\mathbb{Q}$, there is a bottleneck: the algebraic extension $\mathbb{Q}(b)$ is often too big!
More precisely, the degree of the extension used is $[\mathbb{Q}(b) : \mathbb{Q}] = \deg f$. We have just seen (Corollary 1.1.5) that the degree of the extension $\mathbb{Q}(\alpha)$ generated by the coefficients of one absolute factor divides $\mathrm{tdeg}\, f$.

So, even if the algorithm is correct, the computations may take a lot of time (since we look for the coefficients of the absolute factors in a non-minimal field extension) and give non-optimal outputs (since the coefficients of the polynomial in the output will be expressed as roots of $f(a, Y)$).

Example 1.2.6 ([65], page 15)**.** *Consider $f = Y^{10} - 2X^2Y^4 + 4X^6Y^2 - 2X^{10} \in \mathbb{Q}[X, Y]$. We choose $a = 1$, obtaining $f(1, T) = T^{10} - 2T^4 + 4T^2 - 2$ which is square-free. Let b be a root of $f(1, T)$.*

Factoring $f(X, Y)$ on $\mathbb{Q}(b)$, we have the absolute factor

$$F(X, Y) = Y^5 + (b^5 + b^7 + 2b - 2b^3 + b^9)Y^2X + (-2b + 2b^3 - b^5 - b^7 - b^9)X^5.$$

Actually, the absolute factors of f are contained in an extension of $\mathbb{Q}$ of degree 2 instead of 10. If we are able to reconstruct this much smaller extension, the computation of the absolute factor will be much faster (and its presentation much better).

Indeed, an absolute factor of $f(X, Y)$ is

$$G = Y^5 - \sqrt{2}XY^2 + \sqrt{2}X^5 \in \mathbb{Q}(\sqrt{2})[X, Y].$$

Our main aim is to be able to find a better and smaller field extension in which we can factor $f(X, Y)$, namely the one with smaller degree.

1.3 Absolute irreducibility test and Newton Polytope

Before starting the computations of an absolute factorization algorithm, it is wise to check "quickly" if the polynomial is absolutely irreducible, in order to avoid useless computations. Actually, we would like to test a sufficient condition on the polynomial $f(X, Y)$: if it is satisfied, then we do not need to actually perform the factorization algorithm since the polynomial is absolutely irreducible.

The absolute irreducibility test that we are going to present is based on properties of the Newton polytope of a polynomial that we now review.

Definition 1.3.1. *Let* $f(X,Y) = \sum_{i,j} c_{i,j} X^i Y^j \in \mathbb{K}[X,Y]$. *The Newton polytope of* f, *denoted by* P_f, *is the convex hull in* $\mathbb{R}^2$ *of all the points* (i,j) *with* $c_{i,j} \neq 0$.

A point (i,j) *is a* vertex *of* P_f *if it is not on the line segment of any other two points of the polytope.*

We refer to [30] for basic results on absolute irreducibility and Newton polytopes and also for an interesting short history on the subject which goes back to the famous Eisenstein criterion.

Definition 1.3.2. *Denote by* (i_1,j_1), $\ldots$, $(i_l,j_l) \in \mathbb{Z}^2$ *the vertexes of* P_f. *We say that condition* (C) *is satisfied when* $\gcd(i_1,j_1,\ldots,i_l,j_l) = 1$.

Proposition 1.3.3 (Absolute irreducibility criterion)**.** *Let* $f(X,Y)$ *be an irreducible polynomial in* $\mathbb{K}[X,Y]$. *If condition* (C) *is satisfied then* f *is absolutely irreducible.*

Our statement in Proposition 1.3.3 bears similarities with one of Gao's result [30]; but it differs since Gao assumed that P_f should be contained in a triangle when we assume that f is irreducible in $\mathbb{K}[X,Y]$. Although, our condition seems a strong theoretical hypothesis, in practice we can check it very quickly thanks to the algorithms developed in [8] and [52]. The advantage of our criterion is that it applies to a larger variety of polytopes.

In order to prove Proposition 1.3.3, we introduce the Minkowski sum and its properties concerning polytopes.

Definition 1.3.4. *If* A *and* B *are two subsets of the vector space* $\mathbb{R}^n$, *we define their* Minkowski sum *as*

$$A + B = \{a + b | a \in A, b \in B\}.$$

Lemma 1.3.5. *Let* $f,g,h \in \mathbb{K}[X_1,X_2,\ldots,X_n]$ *with* $f = gh$. *Then* $P_f = P_g + P_h$.

Proof. See [63], Theorem VI. □

In particular (see [70]) if we sum up s times the same convex polytope A, then we have that

$$\underbrace{A + \cdots + A}_{s-times} = s \cdot A,$$

where $s \cdot A = \{s \cdot v | v \in A\}$. Furthermore the vertexes $\{v_1,\ldots,v_l\}$ of $s \cdot A$ are exactly $v_i = s \cdot w_i$, where $\{w_1,\ldots,w_l\}$ is the set of vertexes of A.

We now consider the irreducible polynomial $f(X,Y) \in \mathbb{K}[X,Y]$ and its absolute factors $f_1,\ldots,f_s$ in $\overline{\mathbb{K}}[X,Y]$. Observe that thanks to Lemma 1.1.4, we have that $P_{f_i} = P_{f_j}$ for every couple of indexes $i,j \in \{1,\ldots,s\}$.

We can then easily prove Proposition 1.3.3.

Proof of Proposition 1.3.3. Suppose that f is not absolutely irreducible. Let $f_1, \ldots, f_s$ be the absolute factors of f. For what concerns the Newton polytopes, we have that

$$P_f = P_{f_1} + \cdots + P_{f_s} = s \cdot P_{f_1}.$$

Suppose in particular that the vertexes of P_{f_1} are $\{(i_1, j_1), \ldots, (i_l, j_l)\}$. Then we have that the vertexes of P_f are $\{(s \cdot i_1, s \cdot j_1), \ldots, (s \cdot i_l, s \cdot j_l)\}$. But then condition (C) does not hold. □

Corollary 1.3.6. *The number of absolute irreducible factors of a rationally irreducible polynomial $f(X, Y) \in \mathbb{Z}[X, Y]$ divides $\gcd(i_1, j_1, \ldots, i_l, j_l)$.*

Proof. This is a consequence of the proof of Proposition 1.3.3. □

Remark 1.3.7. *This irreducibility criterion first appeared in [14], but with a different proof of Proposition 1.3.3, involving the definition of an appropriate term order.*

In Proposition 1.3.3, we established the validity of our criterion. There is a natural question arising: Does situation (C) happens frequently ?

When the polynomial f is dense, then the coordinates of the vertexes of P_f are $(0, 0)$, $(n, 0)$, $(0, n)$, thus condition (C) is not satisfied and we cannot apply our test. However when f is sparse, in "most" cases, the Newton polytope is not the triangle of the previous situation and a direct use of Proposition 1.3.3 can quickly detect if f is absolutely irreducible.

In the case of dense polynomials, modular computations are used to force a sparsity condition on a reduced polynomial modulo some prime p. For that purpose, we recall Noether's irreducibility theorem (see [60] or [69], Chapter V, Theorem 2A) and an easy consequence concerning the reduction modulo a prime integer.

Theorem 1.3.8 (Noether's irreducibility Theorem)**.** *Let $f(X_1, \ldots, X_n$ be a polynomial in $\mathbb{K}[X_1, \ldots, X_n]$, $\mathbb{K}$ a field. Suppose that the total degree of f is at most $d > 0$ and f is given by*

$$f(X_1, \ldots, X_n) = \sum_{i_1 + \cdots + i_n \leq d} a_{i_i \ldots i_n} X_1^{i_1} \cdots X_n^{i_n}.$$

There exist forms $g_1, \ldots, g_s$ in variables $A_{i_i \ldots i_n}$, $(i_1 + \cdots + i_n \geq d$ such that the polynomial $f(X_1, \ldots, X_n)$ is reducible over $\overline{\mathbb{K}}$ (algebraic closure of $\mathbb{K}$) or of degree $< d$ if and only if

$$g_j(a_{i_1 \ldots i_n}) = 0 \quad 1 \leq j \leq s.$$

The forms g_j depend only on n and d, and are independent of the field $\mathbb{K}$, in the sense that if $\mathbb{K}$ has characteristic 0, they are fixed forms with rational integer coefficients. If $\mathbb{K}$ has characteristic $p \neq 0$, then they are obtained by reducing the integral coefficients modulo p.

As a consequence we have the following proposition

Proposition 1.3.9. *Let* $f(X,Y) \in \mathbb{Z}[X,Y]$ *and* $\overline{f}(X,Y) = f \mod p \in \mathbb{F}_p[X,Y]$. *If* $\mathrm{tdeg}\,(f) = \mathrm{tdeg}\,(\overline{f})$ *and* $\overline{f}$ *is absolutely irreducible, then* f *is absolutely irreducible.*

Now, even if f is dense, the idea is to choose p in order to force $\overline{f}$ to be sparse ; then apply the test to $\overline{f}$ instead of applying it to f.

Let $a_1, \ldots, a_k$ be the coefficients corresponding to the vertexes of P_f and $L = [p_1, \ldots, p_l]$ be the list of the primes dividing at least one of the a_i. Remark that:

$$\forall p_i \in L,\ P_f \neq P_{f \bmod p_i}.$$

Thus even when f is dense, if the coefficients $a_1, \ldots, a_k$ are not all equal to 1, we can get polynomials $f \mod p_i$ such that $P_{f \bmod p_i}$ is not the triangle with vertexes $(0,0)$, $(0,n)$, $(n,0)$.

Example 1.3.10. $f(X,Y) = Y^3 + X^3 + 5X^2 + 3Y + 2$. *Figure 1.1 clearly illustrates the effect of a reduction modulo* p.

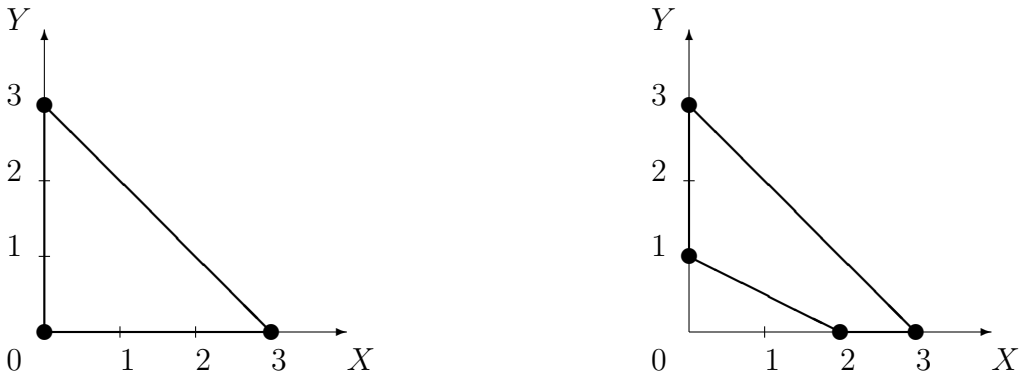

Figure 1.1: Newton polytopes of f and $f \mod 2$

Therefore, thanks to Proposition 1.3.3 and Proposition 1.3.9, absolute irreducibility can be tested with a Las Vegas strategy (i.e. the output of the algorithm is *always* correct). However the output can be "I don't know". More precisely (see Algorithm 2):
For each $p \in L$, test the absolute irreducibility of $\overline{f} \mod p \in \mathbb{F}_p[X,Y]$ with Proposition 1.3.3, and conclude with Proposition 1.3.9.

A last task is to deal with polynomials whose coefficients are 0, 1 or -1 like $f(X,Y) = X^n + Y^n + 1$, because in that case the Newton polytope gives no information, even when one looks at the modular reduction $f \mod p$. The natural strategy is to perform a linear change of coordinates in order to obtain, after reduction, a polynomial satisfying condition (C). This is applied in Algorithm 3.

Algorithm 2 Modular Absolute irreducibility Test

Input: $f(X,Y) \in \mathbb{Z}[X,Y]$, irreducible in $\mathbb{Q}[X,Y]$.

Output: "f is absolutely irreducible" or "I don't know".

Compute P_f and the list L of the primes dividing a coefficient corresponding to a vertex of P_f.
test:=false: $i := 1$:
while test=false **and** $i \leq |L|$ **do**
  $p := L[i]$
  if $\mathrm{tdeg}\,(f \mod p) = \mathrm{tdeg}\,(f)$ **then**
    Compute $P_{f \mod p}$
    if $f \mod p$ satisfies condition (C) **and** $f \mod p$ is irreducible in $\mathbb{F}_p[X,Y]$ **then**
      test:=true;
    end if
  end if
  $i := i + 1$
end while
if test = true **then**
  return "f is absolutely irreducible"
else
  return "I don't know"
end if

Algorithm 3 Modular Absolute irreducibility Test with change of coordinates

Input: $f(X,Y) \in \mathbb{Z}[X,Y]$, irreducible in $\mathbb{Q}[X,Y]$.

Output: "f is absolutely irreducible" or "I don't know".

for p prime between 2 and 101 **do**
  for $(a,b) \in \mathbb{F}_p^2$ **do**
    $f_{a,b}(X,Y) = f(X+a, Y+b) \mod p$
    if $\deg(f_{a,b}) = \deg(f)$ **and** $f_{a,b}$ satisfies condition (C) **then**
      if $f_{a,b}$ is irreducible in $\mathbb{F}_p[X,Y]$ **then**
        return "f is absolutely irreducible"
      end if
    end if
  end for
end for
return "I don't know".

Modular computation is performed in $\mathbb{F}_p$ where p is a prime between 2 and some value, here fixed to 101.

Algorithms 2 and 3 generalize a test given by J.-F. Ragot in [66].

Fact: *Let $f(X,Y) \in \mathbb{K}[X,Y]$ be an irreducible polynomial in $\mathbb{K}[X,Y]$. If there exists $(a,b) \in \mathbb{K}^2$ such that $f(a,b) = 0$ and $\dfrac{\partial f}{\partial X}(a,b) \neq 0$ or $\dfrac{\partial f}{\partial Y}(a,b) \neq 0$, then f is absolutely irreducible.*

Ragot's algorithm tests if $f \mod p$ has a simple root in $\mathbb{F}_p$. Remark that f has a simple root if and only if after a linear change of coordinates, which brings this root at the origin, the Newton polytope of f has at least one of the points $(1,0)$ and $(0,1)$ as vertex while $(0,0)$ is not a vertex.

In that case, condition (C) is satisfied; thus Ragot's test is weaker than our test.

1.4 Modular Factorization

We aim to build a factorization algorithm by extending the analysis and strategy developed for the previous irreducibility test. We keep the notations introduced in Section 1.1 and specially in Lemma 1.1.4.

Our main task is describing an algebraic extension $\mathbb{L} = \mathbb{Q}(\alpha)$ of $\mathbb{Q}$ which contains the coefficients of an absolute factor f_1 of f. We remark again that this is the same that one can obtain through Trager-Traverso algorithm, but the extension we will find is "smaller" then Trager-Traverso's one, and so more suitable for the computation of the factorization.

1.4.1 Algebraic extensions and primitive elements

Since $\mathbb{Q}$ is a separable field, we know that for any algebraic extension of $\mathbb{Q}$, there is a primitive element generating it. Let us see that, for a general choice of $(x_0, y_0) \in \mathbb{Z}^2$, $\mathbb{L} = \mathbb{Q}(f_1(x_0, y_0))$.

Lemma 1.4.1. *Let $f(X,Y) \in \mathbb{Z}[X,Y]$ be a rationally irreducible polynomial of degree n. Let $f_1(X,Y)$ be an absolute factor of $f(X,Y)$, $\deg f_1(X,Y) = m$.*
For almost all $(x_0, y_0) \in \mathbb{Z}^2$ we have $\mathbb{L} = \mathbb{Q}(f_1(x_0, y_0))$.

More precisely, the following estimate on the probability holds:

$$\mathcal{P}\Big(\{(x_0,y_0) \in S^2 \mid \mathbb{L} = \mathbb{Q}(f_1(x_0,y_0))\}\Big) \geq 1 - \frac{n(s-1)}{2|S|} \quad \textit{with } s := n/m,$$

where S is a finite subset of $\mathbb{Z}$.

Proof. We denote by $a_{i,j}$ the coefficients of f_1, so $\mathbb{L} = \mathbb{Q}(a_{i,j})$. Let $\{\sigma_l\}_{l=1,\ldots,s}$ be the set of independent automorphisms of $\mathbb{L}$ fixing $\mathbb{Q}$.

Hence we have:

$$\forall u \neq v, \exists (i,j) \text{ such that } \sigma_u(a_{i,j}) \neq \sigma_v(a_{i,j}). \qquad (*)$$

We consider $D(X,Y) = \prod_{u \neq v} \Big(\sum_{i,j} \big(\sigma_u - \sigma_v\big)(a_{i,j}) X^i Y^j \Big)$.
Property $(*)$ implies that $D(X,Y) \neq 0$. Then there exists $(x_0, y_0) \in \mathbb{Z}^2$ such that $D(x_0, y_0) \neq 0$. This means: for all $u \neq v$, $\sigma_u\big(f_1(x_0,y_0)\big) \neq \sigma_v\big(f_1(x_0,y_0)\big)$. Thus $f_1(x_0,y_0)$ is a primitive element of $\mathbb{L}$ and this gives the desired result.

The probability statement is a direct consequence of Zippel-Schwartz's lemma, applied to $D(X,Y)$, whose degree is bounded by $(ms(s-1))/2 = (n(s-1))/2$. □

Instead of looking for the extension generated by *all* the coefficients of the absolute factors f_1, Lemma 1.4.1 allows us to consider the simple extension of $\mathbb{Q}$ generated by the algebraic number $f_1(x_0,y_0)$, with (x_0,y_0) integers chosen randomly in a big enough finite subset of $\mathbb{Z}$.

Remark 1.4.2. *The polynomial $D(X,Y)$ in the proof of Lemma 1.4.1 is connected to another interesting polynomial: the discriminant, with respect to Z, of the 3-variate polynomial $F(X,Y,Z) = \prod_{j=1}^{s}(Z - f_j(X,Y))$. The discriminant with respect to Z of $F(X,Y,Z)$ is the square of $D(X,Y)$. F has coefficient in $\mathbb{Z}$ because its coefficients are invariant when we permute the f_j's.*

1.4.2 Choice of p

We would like to speed up the computations reducing the coefficients of $f(X,Y) \in \mathbb{Z}[X,Y]$ modulo a prime integer p and performing factorizations modulo p.

We have to carefully choose which are the primes p giving us significant results with respect to the absolute factorization of f.

Theorem 1.4.3 (Chebotarev's density theorem)**.** *Let $q(T)$ be a monic irreducible polynomial of degree s with integer coefficients, with root α, let $\mathbb{K} = \mathbb{Q}(\alpha)$, let $\mathbb{L}$ be the normal closure of $\mathbb{K}$, and let P be a partition $(s_1, s_2, \ldots, s_r)$ of s, i.e., an ordered set of positive integers $s_1 \geq s_2 \geq \cdots \geq s_r$ with $s = s_1 + s_2 + \cdots + s_r$.*
We say that a prime integer is unramified (over the number field $\mathbb{K}$) if it does not divide the discriminant of $q(T)$. Let $\mathcal{S}$ denote the set of unramified primes for $q(T)$. Consider the set $\mathcal{S}_P$ of unramified primes for which $q(T)$ factors as $q_1(T)q_2(T)\cdots q_r(T) \mod p$, where $q_i(T)$ is irreducible modulo p and has degree s_i. Also define the density $\delta(\mathcal{S}_P)$ of primes in $\mathcal{S}_P$ as follows:

$$\delta(\mathcal{S}_P) = \lim_{N \to \infty} \frac{\#\{p \in \mathcal{S}_P : p \leq N\}}{\#\{p \in \mathcal{S} : p \leq N\}}.$$

Now consider the Galois group $Gal(\mathbb{L}/\mathbb{Q})$ of the number field $\mathbb{K}$. Since this is a subgroup of the symmetric group on s elements, every element of $Gal(\mathbb{L}/\mathbb{Q})$ can be represented as a

permutation of s letters, which in turn has a unique representation as a product of disjoint cycles. Now consider the set of elements $Gal(\mathbb{L}/\mathbb{Q})_P$ of $Gal(\mathbb{L}/\mathbb{Q})$ which are a product of disjoint cycles of length $s_1, s_2, \ldots, s_r$.

Then $\delta(\mathcal{S}_P) = \frac{\#Gal(\mathbb{L}/\mathbb{Q})_P}{\#Gal(\mathbb{L}/\mathbb{Q})}$.

Example 1.4.4 ([75]). *Consider the rationally irreducible polynomial*

$$f = X^4 + 3X^2 + 7X + 4.$$

Its discriminant is $17689 = 7^2 \cdot 19^2$, so if we consider all the prime numbers p smaller then 1000, excluding 7 and 19, we have the following percentages of primes p giving a certain splitting patterns for $f \mod p$:

Splitting pattern	*Number of primes p*	*Percentage*
$1, 3$	112	67.5%
$2, 2$	44	26.5%
$1, 1, 1, 1$	10	6%

We can then predict that, if we take a random prime p smaller than 1000, different from 7 and 19, the probability to have splitting pattern $(1, 3)$ modulo p is $2/3$, while for $(2, 2)$ and $(1, 1, 1, 1)$ the predicted probability is respectively $1/4$ and $1/12$. We would also assign probability 0 to the splitting patterns $(1, 1, 2)$ and (4).

Actually, these probabilities are correct: indeed, the Galois group of f is the alternating group A_4, which has 12 elements: the identity which correspond to the splitting pattern $(1, 1, 1, 1)$, 8 permutations that are a product of disjoint cycles of lengths $(1, 3)$ and 3 elements which are a product of disjoint cycles $(2, 2)$. Chebotarev's density theorem validates the probabilities obtained.

If we apply Chebotarev's density Theorem to the minimal polynomial $q(T)$ of $\alpha = f_1(x_0, y_0)$, then we know that there are infinite primes p such that $q(T)$ splits modulo p with at least one linear factor (since the identity permutation has cyclic structure $(1, \ldots, 1)$). Rephrasing, if we choose the partition $P = (s_1, \ldots, s_{r-1}1)$, the probability that a random unramified prime p is in $\mathcal{S}_P$ is $\geq \frac{1}{\#Gal(\mathbb{L}/\mathbb{Q})}$.

However, this is not sufficient for our purposes, we need to find a way to choose a p which ensures a factorization of the minimal polynomial of α with at least one linear factor. Such a prime ensures that also $f(X, Y)$ factors modulo p, but we have to pay attention also to the fact that the chosen p preserves the number of absolute factors of f.

Definition 1.4.5. *We say that the prime integer p gives a* bad reduction *of $f(X, Y)$ if the number of absolute factors of $f(X, Y) \mod p$ differs from the number of absolute factors of $f(X, Y)$; otherwise, we say that p gives a* good reduction.

Proposition 1.4.6. *Let $f(X,Y)$ be a rationally irreducible polynomial, monic in Y. Then there is a finite number of prime integers p giving a bad reduction of $f(X,Y)$.*

Furthermore, if $d(X) = disc_Y(f(X,Y))$, $d_1(X) =$ square-free part of $d(X)$, $D = disc_X(d_1(X))$, then the set of prime integers p giving a bad reduction of f is contained in the set of prime divisors of D.

Proof. The finiteness of the set of p giving bad reductions comes from a theorem of E. Noether (see [60]). For the characterization using D, we can say with other words that $f(X,Y)$ has a good reduction $\bmod p$ if $d(X)$ and $d(X) \mod p$ have the same number of distinct roots. For the proof of this fact, see [79]. Finally, for another proof, see [84]. □

Example 1.4.7. *Consider the bivariate polynomial $f(X,Y) = -20X^2 + 73XY + 80Y^2 - 29X + 85Y - 84$. f is rationally irreducible and absolutely irreducible, but if we choose $p = 7$,*

$$f(X,Y) = (X + 6Y)(X + 4Y + 6) \mod p.$$

The constant D of Proposition 1.4.6 is in this case 282403520 and so the primes giving bad reductions are included in the set $\{2, 5, 7, 139, 907\}$.

Lemma 1.4.8. *Let $f(X,Y) \in \mathbb{Z}[X,Y]$, and let $\mathcal{B}$ be a positive integer. There exists $(x_0, y_0) \in \mathbb{Z}^2$ and $p \in \mathbb{Z}$ prime such that p divides $f(x_0, y_0)$ and p doesn't divide $\mathcal{B}$.*

Proof. We can reduce to the case of one variable and use the classical argument of Dirichlet for proving that the set of prime numbers is infinite.

Consider the polynomial $f(X) \in \mathbb{Z}[X]$, $\deg f \geq 1$. Consider x_1 such that the constant term $c := f(x_1)$ is not zero.

Set $\tilde{f}(X) = f(X - x_1)$, so c is the constant term of $\tilde{f}(X)$. Consider $\tilde{f}(c\mathcal{B}X) = c(1 + \mathcal{B}Xq(X))$, where $q(X) \in \mathbb{Z}[X]$ is not zero (otherwise $degf < 1$). We can find $x_0 \in \mathbb{Z}$, $x_0 \neq 0$ such that $\mathcal{B}x_0q(x_0) \neq 0$. Then, a prime p dividing $1 + \mathcal{B}x_0q(x_0)$ does not divide $\mathcal{B}$ and we are done. □

Thanks to this lemma, we know that there exists a point $(x_0, y_0) \in \mathbb{Z}^2$ such that there is a p dividing $f(x_0, y_0)$ and not dividing the constant D of Lemma 1.4.6. We can then rely on randomness to avoid a p giving a bad reduction or we can proceed in a deterministic way, computing the integer D and choosing a p not dividing D.

The next step in the choice of p is to force $f(X,Y)$ to factor in $\mathbb{Z}/p\mathbb{Z}[X,Y]$, in order to have an "image" modulo p of an absolute factor of f.

Lemma 1.4.9. *Let $M(T) \in \mathbb{Z}[T]$ be a polynomial and p a prime number such that p divides $M(0)$, p does not divide the discriminant of $q(T)$ and $p > \deg(M)$.*
Then there exists a root in $\mathbb{Q}_p$ of $M(T)$, considered as a polynomial in $\mathbb{Q}_p[T]$.

Proof. Since $M(0) = 0 \mod p$ and $p \nmid disc(q(T))$, 0 is also a root of $M_1(T) = \frac{M(T)}{\gcd(M(T),M'(T))}$ in $\mathbb{F}_p$. As $p > \deg(M)$, we have $M_1'(0) \neq 0$ in $\mathbb{F}_p$ and we can lift this root in $\mathbb{Q}_p$ by Hensel's liftings. This gives a root of $M_1(T)$ in $\mathbb{Q}_p$, thus a root of $M(T)$ in $\mathbb{Q}_p$. □

Lemma 1.4.9 allows us to consider a number field $\mathbb{Q}(\alpha)$ as a subfield of $\mathbb{Q}_p$, for a well-chosen prime p. Indeed, if $q(T)$ is the minimal polynomial of α, then with a big enough integer c we can find a prime number p such that the polynomial $q(T + c)$ satisfies the hypothesis of Lemma 1.4.9. Thus we can consider $\alpha + c$ in $\mathbb{Q}_p$, then $\mathbb{Q}(\alpha) \subset \mathbb{Q}_p$. Later we will consider the modular factorization of $f(X, Y)$. We can consider it as an "approximate" factorization of f in $\mathbb{Q}(\alpha)$ with the p-adic norm (see Chapter B of the Appendix for some details on the field of p-adic numbers). Then this factorization gives information about the absolute factorization.

We then have a strategy to choose a prime p such that the factorization of $f \mod p$ is a first approximation of the absolute factorization of f, that is

$$f \mod p = F \cdot G \mod p \qquad \text{with } \deg F = \deg f_1.$$

We can choose a point with integer coordinates (x_0, y_0). We know that for a general choice of this point, $\alpha = f_1(x_0, y_0)$ generates the algebraic extension of $\mathbb{Q}$ in which there are the coefficients of one of the absolute factors of f. The minimal polynomial of α is $q(T) = \prod_{i=1}^{s}(T - \alpha_i)$.
Now we observe that $f(x_0, y_0) = f_1(x_0, y_0) \cdots f_s(x_0, y_0) = \alpha_1 \cdots \alpha_s$ with $\alpha_1 = \alpha$. This means that $f(x_0, y_0)$ is equal to the constant term of the minimal polynomial of α.
So, we will choose a random point with integer coefficients (x_0, y_0) and a prime p dividing $f(x_0, y_0)$. If p is big enough to respect the hypothesis of Lemma 1.4.9 applied to $q(T)$, we have a root of $q(T)$ in $\mathbb{Q}_p$ and so we also have an absolute factor of f whose coefficients are in $\mathbb{Q}_p$ (since the coefficients of f_1 depend only on α).
This means that $f \mod p$ splits as $F \cdot G \mod p$ with $\deg f_1 = \deg F$. Relying on the good behaviour of a general point (x_0, y_0) (Lemma 1.4.1) and the good behaviour of a general prime p with respect to good reductions (Proposition 1.4.6), we have that $f \mod p = F \cdot G \mod p$ is a p-adic approximation of the factorization $f = f_1 \cdot (f_2 \cdots f_s)$.

1.4.3 Recognition strategy

We assume that we chose a good prime p, such that $\mathrm{tdeg}\,(f) = \mathrm{tdeg}\,(f \mod p)$ and $f \mod p$ factors as $f(X, Y) = F^{(1)}(X, Y) \cdot G^{(1)}(X, Y) \mod p$ where $F^{(1)}$ is exactly the image modulo p of an absolute factor f_1 of f.

In order to find the splitting field of $f(x_0, Y)$, relying on Proposition 1.4.1, we need to compute $q(T)$, the minimal polynomial with integer coefficients of $\alpha := f_1(x_0, y_0)$.

Starting from a factorization $f(x_0, Y) = F^{(1)}(x_0, Y)G^{(1)}(x_0, Y) \mod p$, we lift it through Hensel Lifting (Theorem B.5.1) to the level of accuracy p^λ. We then consider the p-adic approximation $\overline{\alpha} := F^{(\lambda)}(x_0, y_0)$ of α. Using a "big enough" level of accuracy λ, we can compute the minimal polynomial of α from $\overline{\alpha}$.

We denote with $\|\cdot\|$ the *Euclidean norm* of a polynomial (that is of its vector of coefficients) and with $\|\cdot\|_\infty$ the *norm at infinity*.

Lemma 1.4.10. *[[81], Lemma 16.20] Let $f, g \in \mathbb{Z}[X]$ have positive degrees n_1, n_2 respectively, and suppose that $u \in \mathbb{Z}[X]$ is nonconstant, monic, and divides both f and g modulo m for some $m \in \mathbb{N}$ with $\|f\|^{n_2}\|g\|^{n_1} < m$.*
Then $\gcd(f, g) \in Z[X]$ is nonconstant.

Proof. Suppose that $\gcd(f, g) = 1$ in $\mathbb{Q}[X]$. Then there exist $s, t \in \mathbb{Z}[X]$ such that $sf + tg = res(f, g) \mod m$, by [81], Corollary 6.21. Since u divides both f and g modulo m, it divides $res(f, g)$ modulo m. But u is monic and nonconstant, and thus $res(f, g) = 0 \mod m$. Since $|res(f, g)| < \|f\|^{n_2}\|g\|^{n_1} < m$, by [81], Theorem 6.23, it follows that $res(f, g)$ is zero. This contradiction to our assumption shows that $\gcd(f, g) \in \mathbb{Q}[x]$ is nonconstant. By [81], Corollary 6.10, the gcd of f and g in $\mathbb{Z}[X]$ is also nonconstant. □

Proposition 1.4.11. *Consider $\overline{\alpha} = F^{(\lambda)}(x_0, y_0)$, $0 \leq \overline{\alpha} \leq p^\lambda - 1$ constructed above, a positive integer Q bounding the size of the coefficients of $q(T)$, $Q \geq \|q(T)\|_\infty$, and a positive integer $\lambda \geq \log_p(2^{s^2/2}(s+1)^s Q^{2s})$.*

Then we can compute the minimal polynomial $q(T)$ of α using the LLL algorithm on an integer lattice whose basis is given using $\overline{\alpha}$ and p^λ.

Proof. We apply the same construction of [81], Section 16.4, for detecting rational factors of univariate polynomials.

We consider the polynomials

$$\{T^i(T - \overline{\alpha}) | i = 0, \ldots, s-1\} \cup \{p^\lambda\}.$$

We write as usual

$$T^i(T - \overline{\alpha}) = T^{i+1} - \overline{\alpha}T^i = \sum_{j=0}^{s} t_j T^j,$$

where, in this case, $t_j \neq 0$ for $j \in \{i+1, i\}$ and $t_j = 0$ otherwise. Then the associated vector for the polynomial $T^i(T - \overline{\alpha})$ is

$$b_i = (t_s, \ldots, t_0).$$

For the constant polynomial p^λ, we associate the vector $\tilde{b} = (0, \ldots, 0, p^\lambda)$. We can construct the $(s+1) \times (s+1)$ matrix B whose columns are the b_i, $i = 0, \ldots, s-1$ and $\tilde{b}$:

$$B = \begin{bmatrix} 1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ -\overline{\alpha} & 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & -\overline{\alpha} & 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & -\overline{\alpha} & 1 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & -\overline{\alpha} & 1 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & -\overline{\alpha} & p^\lambda \end{bmatrix}$$

If we consider a point g of the integer lattice $\Lambda(B) \subseteq \mathbb{R}^{s+1}$ generated by the columns of the matrix B, we can write its components with respect to the standard basis of $\mathbb{R}^{s+1}$

$$g = \sum_{i=0}^{s-1} g_i b_i + \tilde{g}\tilde{b} = (g_{s-1}, g_{s-2} - \overline{\alpha} g_{s-1}, \dots, g_0 - \overline{\alpha} g_1, \tilde{g}p^\lambda - \overline{\alpha} g_0),$$

and associate a polynomial:

$$G(T) = g_{s-1}T^s + (g_{s-2} - \overline{\alpha} g_{s-1})T^{s-1} + \cdots + (g_0 - \overline{\alpha} g_1)T + \tilde{g}p^\lambda - \overline{\alpha} g_0 =$$

$$= S(T)(T - \overline{\alpha}) + \tilde{g}p^\lambda \quad \text{with} \quad S(T) = \sum_{i=0}^{s-1} g_i T^i.$$

So if $g \in \Lambda(B)$, the associated polynomial $G(T)$ has degree $\leq s$ and it is divisible by $(T - \overline{\alpha})$ modulo p^γ.

The *vice versa* holds: if $G(T)$ is a polynomial of degree at most s and $G(T) \mod p^\lambda$ is divisible by $(T - \overline{\alpha})$, then we can write

$$G(T) = S^*(T)(T - \overline{\alpha}) + R^*(T)p^\gamma \quad \text{with } \deg S^*(T) \leq s - 1 \text{ and } \deg R^*(T) \leq s.$$

Using Euclidean division, we obtain $R^*(T) = S^{**}(T)(T - \overline{\alpha}) + Rp^\gamma$ with $\deg S^{**} \leq s - 1$ and R a costant. We define $S(T) := S^*(T) + p^\gamma S^{**}(T)$. We then have that

$$G(T) = S(T)(T - \overline{\alpha}) + Rp^\gamma,$$

that is, $G(T)$ can be written as a point of the lattice $\Lambda(B)$.

So if we consider the matrix B and we apply the LLL algorithm, we obtain as first vector of the reduced basis a "short"vector representing a polynomial $G(T)$ with "small" norm such that $G(T)$ has degree s and $G(T) \mod p^\lambda$ is divisible by $(T - \overline{\alpha})$. Using the hypothesis $\lambda \geq \log_p(2^{s^2/2}(s+1)^s Q^{2s})$ we can apply Lemma 1.4.10: we then have that $q(T)$ and $G(T)$ have a non-constant $\gcd$. But since $q(T)$ is irreducible and $\deg q(T) = \deg G(T)$, we have that $q(T) = G(T)$. □

Remark 1.4.12. *Another lattice, inspired by [83], Lecture IX, Section 6, and [47], allows us to compute the minimal polynomial $q(T)$ of α starting from its p-adic approximation $\overline{\alpha}$.*

Consider the lattice $\Lambda(A)$ in $\mathbb{R}^{s+2}$ generated by the columns $a_0, a_1, \ldots, a_{s-1}, a_s, \tilde{a}$ of the matrix

$$A = \begin{bmatrix} c & c\overline{\alpha} & c\overline{\alpha}^2 & \cdots & c\overline{\alpha}^{s-1} & c\overline{\alpha}^s & cp^\lambda \\ 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & 0 \end{bmatrix}$$

with $c >> 0$ positive integer.

If $q(T) = \sum_{i=0}^{s} q_i T^i$ is the minimal polynomial of α, $Q \geq \|q(T)\|_\infty$, choose $\lambda \geq \log_p(2^{s^2/2}(s+1)^s Q^{2s})$ (as in Lemma 1.4.11), and $c \geq 2^{(s+1)/2}\sqrt{s+1}Q$. Then the vector $\sum_{i=0}^{s} q_i a_i$ is the smallest vector in the lattice $\Lambda(A)$. Indeed, observe that any vector $\vec{\gamma} \in \Lambda(A)$ such that

$$c(\gamma_0 + \gamma_i\overline{\alpha} + \cdots + \gamma_s\overline{\alpha}^s + \tilde{\gamma}p^\lambda) \neq 0$$

has euclidean norm bigger than the euclidean norm of $q(T)$. Furthermore, thanks to the choice of λ, if $\vec{\gamma}$ is such that $c(\gamma_0 + \gamma_i\overline{\alpha} + \cdots + \gamma_s\overline{\alpha}^s + \tilde{\gamma}p^\lambda) = 0$, using the same arguments used in the proof of Lemma 1.4.11, then the polynomial $\sum_{i=0}^{s} \gamma_i T^i$ is an integer multiple of $q(T)$ and obviously its euclidean norm is bigger than the one of $q(T)$.
Then, if we apply the LLL algorithm to $\Lambda(A)$, the short vector found must respect inequality $i)$ of Lemma A.3.5, so its first component has to be 0 and thanks to the choice of λ, we have a polynomial which has a root in α. Since it has degree s, its primitive part is $q(T)$.

To establish the level of accuracy λ in Proposition 1.4.11 (and to fix c in Remark 1.4.12), we need a bound on the size of the coefficients of the minimal polynomial of α, $q(T)$. Remember that

$$q(T) = \prod_{i=1}^{s}(T - \alpha_i) = T^s + \sigma_1(\tilde{\alpha}) + \cdots + \sigma_{s-1}(\tilde{\alpha})T + \sigma_s(\tilde{\alpha}),$$

where $\sigma_i(\tilde{\alpha})$ is the i-th symmetric function in the $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_s$.

Observe that

$$|\sigma_k(\tilde{\alpha})| \leq \sum_{\tau \in \mathcal{S}_k} |\alpha_{\tau(1)}| \cdots |\alpha_{\tau(k)}| \leq \sum_{\tau \in \mathcal{S}_k} \prod_{j=1}^{m} |y_j^{\tau(1)}| \cdots \prod_{j=1}^{m} |y_j^{\tau(k)}|,$$

where $f_l(x_0, Y) = \prod_{j=1}^{m}(Y - y_j^{(l)})$ and $f(x_0, Y) = \prod_{i=1}^{s} f_l(x_0, Y)$.

As a bound on the coefficients of $f(x_0, Y)$ gives a bound on the $y_j^{(l)}$ ([81]), a bound on the coefficients of $f(x_0, Y)$ gives a bound for $\|q(T)\|_\infty$.

In practice, for "early detection", we rely on Proposition 1.4.11 replacing Q by

$$Q_1 = \|f(x_0, Y)\|_\infty.$$

Remark 1.4.13. *We are not assuming that $f(X, Y)$ is monic, so we have to face two problems:*

1. Leading coefficient problem*: we cannot apply Hensel lifting in its "classical" form, because we need to have a factorization $f(x_0, Y) = f_1(x_0, Y)h(x_0, Y) \mod p$ in which $f_1(x_0, Y)$ or $h(x_0, Y)$ is monic;*

2. *in practical use of this construction of the minimal polynomial of α, we will avoid to lift the factorization until the level γ of Proposition 1.4.11 (this bound is usually very pessimistic): however, in this way we are not sure that the primitive part of the polynomial $G(T)$ is actually $q(T)$. We then need a quick method to check if we found a good candidate to define the field extension or if we have to lift the factorization to a higher level of accuracy.*

Consider $f(x_0, Y) = \sum_{i=0}^{n} \phi_i Y^i$.

For what concerns the leading coefficient problem*, we can simply consider the "modified" linear Hensel Lifting (see [31], Algorithm 6.1). In this way we can lift the factorization modulo p, but the coefficients involved in the computations are bigger, since actually we lift a factorization of $\phi_n \cdot f(x_0, Y)$, obtaining a factor that we call $\tilde{f}_1(Y)$.*

For what concerns the second problem, we have to understand how the roots of a factor of $f(x_0, Y)$ are in connection with the coefficients of $q(T)$ and $\tilde{f}_1(Y)$. We call q_s the leading coefficient of the polynomial $q(T)$.

If $f_1(Y)$ is the true factor of $f(x_0, Y)$, then the product of its roots is simply $\beta := (-1)^{\deg \tilde{f}_1(Y)} \tilde{f}_1(y_0)/\phi_n$.

Then the product of the conjugated of β is simply $q(0)/q_s$, but this is also the product of all the roots of $f(x_0, Y)$. So we have the following relation $\frac{q(0)}{q_s} = (-1)^s \frac{f(x_0, y_0)}{\phi_n}$.

When we apply the LLL algorithm to $\bigwedge(B)$ we can then proceed as follows: if the obtained polynomial $G(T)$ satisfies

$$\frac{G(0)}{G_s} = (-1)^s \frac{f(x_0, y_0)}{\phi_n} \qquad \text{with } G_s \text{ leading coefficient of } G(T) \tag{1.4.1}$$

then we will try to factor $f(x_0, Y)$ in the algebraic extension defined by the primitive part of $G(T)$, that is $\mathbb{Q}[T]/p.p.G(T)$. If $G(0)/G_s \neq (-1)^s f(x_0, y_0)/\phi_n$, then we have to rise the

level of approximation of the Hensel lifting and then apply again LLL to the new lattice and test again.

In this way we have a necessary condition that can help us to recognize the minimal polynomial of α.

1.5 Absolute factorization algorithm

We use the results and methods of the previous section to compute an absolute factor f_1 of f (i.e. a representation of the field $\mathbb{L}$ of its coefficient and the coefficients).

To ease the presentation, we rely on the practical evidence that for random integer value x_0, $f(x_0, Y)$ is irreducible. In Section 1.5.2 we will present a variant using a weaker condition.

Proposition 1.5.1. *Algorithm 4 gives a correct answer.*

Proof. Since it is a Las Vegas algorithm, Algorithm 4 is probably fast and always correct but the answer can be "I don't know". So we just have to check that a given positive answer is correct.

The starting point of the algorithm, as in the irreducibility test, is to determine a prime p such that the reduction modulo p kills the evaluation of f on an integer point (x_0, y_0). Then the constant term of the minimal polynomial of $\alpha := f_1(x_0, y_0)$ vanishes modulo p. Such a p is easily found. However we rely on randomness to expect with a good probability that $\mathbb{L} = \mathbb{Q}(\alpha)$ and that f has good reduction modulo p (using Proposition 1.4.6 and Lemma 1.4.9).

In Algorithm 4, we inserted some checks and a loop to change p if it is an "unlucky" choice. The algorithm can be made deterministic (but less efficient) by considering a large testing set for (x_0, y_0) and take p not dividing the constant of Lemma 1.4.6, to avoid bad reduction. We would be able to do this thanks to Lemma 1.4.8.

The output of the algorithm, the factor f_1, is irreducible in $\mathbb{L}[X, Y]$. Indeed, $f_1(x_0, Y) = F_1(x_0, Y)$ and $F_1(x_0, Y)$ is irreducible in $\mathbb{L}[Y]$ because of the irreducibility of $f(x_0, Y)$ in the Preprocessing Step. Furthermore, the extension $\mathbb{L}$ is minimal. Indeed, at the end of the algorithm we have $\deg_Y f_1 = m$, $\deg q = s$ and $s \cdot m = n$ (see the definition of s in Step 2). □

1.5.1 Parallel version of the Algorithm

In step (17) of Algorithm 4 we perform a factorization of $f(x_0, Y)$ in the polynomial ring $\mathbb{L}[Y]$. Then in Step (21) we use Hensel liftings to reconstruct the factor f_1. If we use parallel calculus in these steps, we can perform $(m + 1)$ Lagrange interpolations to reconstruct the

Algorithm 4 Absolute Factorization algorithm

Input: $f(X,Y) \in \mathbb{Z}[X,Y]$, irreducible in $\mathbb{Q}[X,Y]$of degree n, a finite subset S of $\mathbb{Z}^2$.

Output: $q(T) \in \mathbb{Q}[T]$ minimal polynomial of α defining the algebraic extension $\mathbb{L} = \mathbb{Q}(\alpha) = \mathbb{Q}[T]/q(T)$ and $f_1(X,Y) \in \mathbb{L}[X,Y]$ an absolute irreducible factor of f, or "I don't know"

Preprocessing: Choose randomly $(x_0, y_0) \in S^2$, such that $f(x_0, Y)$ is irreducible.

1: Choose a prime p dividing $f(x_0, y_0)$ such that $\mathrm{tdeg}\,(f \mod p) = \mathrm{tdeg}\,(f)$.
2: Factorize f in $\mathbb{F}_p[X,Y]$.
3: **if** $f \mod p$ is irreducible and satisfies an absolute irreducibility test **then**
4: **return** "f is absolutely irreducible", $f_1 := f$ and $q(T) := T$
5: **else**
6: **if** $f \mod p$ is irreducible and not absolutely irreducible **then**
7: go to the Preprocessing step.
8: **else**
9: $f = F \cdot G$ where F is one of the irreducible factor in $\mathbb{F}_p[X,Y]$ with smallest degree m, check that $s := \frac{\mathrm{tdeg}\,(f)}{m}$ is an integer else go to the Preprocessing step.
10: **end if**
11: **end if**
12: Lift the factorization to $f(x_0,Y) = F^{(\lambda)}(x_0,Y)G^{(\lambda)}(x_0,Y) \mod p^\lambda$; λ is chosen according to Proposition 1.4.11 and Remark 1.4.13.
13: Define $\overline{\alpha} := F^{(\lambda)}(x_0, y_0) \in \mathbb{Z}/p^\lambda\mathbb{Z}$. Find, using the lattice described in section 1.4.3 and the LLL algorithm, the polynomial $q(T)$.
14: **if** $q(T)$ does not satisfy (1.4.1) **then**
15: go back to step 12 and double λ.
16: **end if**
17: Denote by α a root of $q(T)$ (i.e. the command RootOf in Maple) then factorize $f(x_0,Y)$ in $\mathbb{Q}(\alpha)[Y] = \mathbb{L}[Y]$ and denote by $F_1(x_0,Y)$ a factor with degree m and with $F_1(x_0,y_0) = \alpha$.
18: **if** there is not such a factor **then**
19: go to the Preprocessing step.
20: **end if**
21: Perform m X-adic Hensel liftings on $f(x_0,Y) = F_1(x_0,Y)F_2(x_0,Y)$ to determine a candidate for $f_1(X,Y)$ in $\mathbb{L}[X,Y]$ and check that it divides $f(X,Y)$.
22: **if** it does not divide $f(X,Y)$ **then**
23: go to the Preprocessing step.
24: **else**
25: **return** $q(T)$ and $f_1(X,Y)$
26: **end if**.

factor f_1. We have to assume that in the factorization of $f(x_0, Y)$ in $\mathbb{L}[Y]$ there is only one factor of degree m. This is not always verified, for instance if the extension $\mathbb{L}$ is normal we may have several factors of the same degree m.

We write the absolute factor f_1 as

$$f_1(X,Y) = Y^m + \sum_{k=0}^{m-1} \sum_{i+j=k} a_{i,j}^{(1)} X^i Y^j = Y^m + \sum_{j=0}^{m-1} b_j(\alpha, X) Y^j,$$

where $b_j(Z, X) \in \mathbb{Q}[Z, X]$ of degree $\leq m - j$ and α is a root of the polynomial $q(T)$ found in step (4).

We then want to find the polynomials $b_j(\alpha, X)$.

We substitute steps from (17) to (21) of Algorithm 4 with the procedure of Algorithm 5.

Algorithm 5 Parallel Version of Algorithm 4

1: Denote by α a root of $q(T)$ (i.e. the command RootOf in Maple).
2: Choose points $x_1, \ldots, x_m \in \mathbb{Z}$, $x_i \neq x_0$ for $i = 1, \ldots, m$ such that $f(x_i, Y)$ is rationally irreducible.
3: Compute the factorization of $f(x_i, Y)$ in $\mathbb{L}[Y]$ and choose $F_{1,0}(Y)$ form the factorization of $f(x_0, Y)$ as in step 17 of the algorithm and $F_{1,j}(Y)$ a factor of minimal degree m in the factorization of $f(x_j, Y)$.
4: Write $F_{1,j}(Y)$ as
$$F_{1,j} = \sum_{i=0}^{m} \gamma_{i,j} Y^j \text{ with } \gamma_j \in \mathbb{L}.$$
5: Construct the polynomials $b_j(\alpha, X)$ of degree j using Lagrange interpolation [9, Section 3.1] on the set of nodes $\gamma_{0,j}, \ldots, \gamma_{j,j}$, obtaining a candidate for $f_1(X, Y)$.
6: **if** it does not divide $f(X, Y)$ **then**
7: go to the Preprocessing step
8: **end if**

The advantage of Algorithm 5 is that in this way this part of the algorithm can be naturally parallelized and does not saturate the memory.

1.5.2 Hilbert's Irreducibility Theorem

In the preprocessing step we check that $f(x_0, Y)$ is irreducible. This situation happens very often in practice. With a more theoretical point of view, we know that there exists an infinite number of $x_0 \in \mathbb{Z}$ such that $f(x_0, Y)$ is irreducible, thanks to Hilbert's irreducibility theorem. There exist bounds for this theorem but unfortunately they are very big, see [20].

Here we now use a weaker condition on the choice of (x_0, y_0) that allows us to reconstruct the factor $f_1(X, Y)$ even if $f(x_0, Y)$ is not rationally irreducible.

Choose an integer point $(x_0, y_0) \in \mathbb{Z}^2$ such that x_0 is not a root of the polynomial $\Delta(X) = \mathrm{disc}_Y(f(X,Y))$ and choose an integer p such that $\Delta(x_0) \mod p \neq 0$. With this choice of (x_0, y_0) we are sure that the univariate polynomial $f(x_0, Y)$ has no multiple roots in $\mathbb{Q}$ nor in $\mathbb{F}_p$.

We do not assume that $f(x_0, Y)$ is rationally irreducible. We compute the factorization modulo p

$$f(X,Y) = F(X,Y) \cdot G(X,Y) \in \mathbb{F}_p[X,Y] \quad \deg F = m.$$

Thanks to the choice of p as in Step (1) of Algorithm 4, $F(X,Y)$ is generically equal modulo p to the researched absolute factor $f_1(X,Y)$ of f.

After applying step (17), we get the following factorization

$$f(x_0, Y) = \psi_1(Y) \cdots \psi_r(Y) \in \mathbb{Q}(\alpha)[Y] \tag{1.5.1}$$

and need to find the set of indexes $I \subseteq \{1, \ldots, r\}$ such that

$$\prod_{i \in I} \psi_i(Y) = f_1(x_0, Y). \tag{1.5.2}$$

We reduce modulo p the equalities (1.5.1) and (1.5.2). We obtain that $j \in I$ if and only if $\psi_j \mod p$ divides $F(x_0, Y) \mod p$.

1.6 Examples and practical complexity

We tested our algorithm on several examples, using (probably non-optimal) routines implemented in Maple 10.

We focused on the construction of the minimal polynomial $q(T)$ of α, that is on the construction of the splitting field $\mathbb{Q}(\alpha)$; in fact the last part of the algorithm (X-adic Hensel lifting or Lagrange interpolation) depends strongly on the used software.

The procedures, data and Maple files of several examples are available at
http://math.unice.fr/∼cbertone/

Here we list some remarks about both the strong and the weak points of our algorithm arising from the computed examples.

• In general the algorithm is quite fast: it took around 30 sec (factorization modulo p, Hensel lifting, construction of the minimal polynomial) to compute the polynomial $q(T)$ starting from a polynomial of degree 200, with 10 absolute factors of degree 20 each.

• If possible, it seems to be a good idea to choose a "small" prime p (in this way we can gain some time in the modular factorization). If the integers dividing $f(x_0, y_0)$ are quite big, it may be better to go back to the preprocessing step.

• On some examples of high degree, most of the time is spent for the construction of the minimal polynomial from the approximation $\overline{\alpha}$. In our tests, we used the LLL function of

Maple, but we may speed up this part of the computation using faster algorithms for LLL (for example, see [59] and [71]).

• For the computation of the p-adic Hensel Lifting, we implemented a small procedure in Maple, both for the linear and the quadratic one, which can deal also with non-monic polynomials ([81], Algorithm 15.10).

Benchmark

We consider random polynomials $g_1 \in \mathbb{Q}[X, Y, Z]$ and $g_2 \in \mathbb{Q}[Z]$, of degrees d_1 and d_2 resp. both rationally irreducible. We compute $f(X, Y) = Res_Z(g_1, g_2)$. In this way we obtain an irreducible polynomial $f(X, Y) \in \mathbb{Q}[X, Y]$, monic in Y, of degree $d_1 \cdot d_2$ with d_2 absolutely irreducible factors each of degree d_1.

The polynomials g_1 and g_2 used are listed in the file "Polynomials.mws".

Here we summarize the time needed to obtain $q(T)$, the minimal rational polynomial of α, such that the absolute factors of $f(X, Y)$ are in $\mathbb{L}[X, Y]$, $\mathbb{L} = \mathbb{Q}(\alpha) = \mathbb{Q}[T]/q(T)$ and we made a few remarks about the strategy one may adopt (for instance the choice of the prime).

In almost all of the examples, we computed the Hensel lifting both with the linear and the quadratic algorithm, this is why we always chose as level of accuracy a power of 2.

In the first 2 examples, we also computed the factorization of $f(x_0, Y)$ in $\mathbb{Q}(\alpha)$.

In the first example, we computed the factor $f_1(X, Y)$ using Lagrange Interpolation.

To repeat the examples, one need to change at the beginning of each Maple file the location of the file "proc.txt", in which there are (non-optimal) implementations for linear and quadratic Hensel Lifting (for non monic polynomials) and a procedure to compute the minimal polynomial of a p-adic approximation of α using the LLL algorithm, using the lattice of Proposition 1.4.11.

The names of kind "Example1.2.mws" refer to the Maple files on the webpage.

Example 1.6.1. *$f(X, Y)$ rational irreducible polynomial of degree 50 with 5 absolute factors of degree 10.*

We needed 1.5 sec to construct the example and factor $f(0, 0)$. We constructed the minimal polynomial defining the field extension for 2 different choices of p.

Example1.1.mws: we chose $p = 11$.

• *Time to factor $f(X, Y) \mod p$:* 0.131 *sec.*

The estimation of the level of accuracy that ensures the correct computation of $q(T)$ was in this case 338; we chose to lift the factorization to the level p^{256}.

• *Time to lift the factorization $f(0, Y) = g_1(0, Y)g_2(0, Y) \mod p$ to a factorization $\mod p^{256}$, using:*

Linear Hensel Lifting: less than 1 *sec*
Quadratic Hensel Lifting: less than 0.07 *sec.*

• *Time to find the minimal polynomial of* α *through its approximation* $\mod p^{256}$ *using* LLL*:* 0.22 *sec.*

We can complete the algorithm using the procedure in Algorithm 5:
we chose 10 nodes $x_1 \ldots, x_{10}$ *randomly and factor the polynomials* $f(x_j, Y)$ *in* $\mathbb{Q}(\alpha)[Y]$*; the longest of these factorization took about* 219 *sec. Then we used Lagrange Interpolation and obtained* $f_1(X, Y)$*.*
Example1.3.mws: if we use the software Pari GP*, applying the function* polred() *to the obtained polynomial* $q(T)$*, we get* $q_1(Z)$ *which defines the same algebraic extension as* $q(T)$ *but has smaller coefficients. In this way, the factorization of* $f(0, Y)$ *in* $\mathbb{Q}(\alpha)$ *took only 8 sec, but the computation of the polynomial* $q_1(Z)$ *in Pari GP took more than 360 sec!*

Example 1.6.2. $f(X, Y)$ *rational irreducible polynomial of degree 400 with 20 absolute factors of degree 20.*

We needed around 1260 *sec to construct the example and factor* $f(0, 0)$*.*

Example6.1.mws: we chose $p = 53259165137$*.*

• *Time to factor* $f(X, Y) \mod p$*:* 1924 *sec.*

The estimation of the level of accuracy that ensures the correct computation of $q(T)$ *was in this case 398; we chose to lift the factorization to the level* p^{256}*.*

• *Time to lift the factorization* $f(0, Y) = g_1(0, Y)g_2(0, Y) \mod p$ *to a factorization* $\mod p^{256}$*, using*
Linear Hensel Lifting: less than 365 *sec*
Quadratic Hensel Lifting: less than 39 *sec.*

• *Time to find the minimal polynomial of* α *through its approximation* $\mod p^{256}$ *using* LLL*:* 1024 *sec.*

In order to compare the time needed for the construction of $q(T)$ *computing modulo a "small" prime, we considered also the case with* $p = 89$ *dividing* $f(-1, 0)$*. In this case we obtained (Example6.2.mws):*

• *Time to factor* $f(X, Y) \mod p$*:* 127 *sec.*

The estimation of the level of accuracy that ensures the correct computation of $q(T)$ *is in this case 2194; we choose to lift the factorization to the level* p^{1024}*.*

• *Time to lift the factorization* $f(0, Y) = g_1(0, Y)g_2(0, Y) \mod p$ *to a factorization* $\mod p^{1024}$*, using*
Linear Hensel Lifting: 737 *sec*
Quadratic Hensel Lifting: 24 *sec.*

• *Time to find the minimal polynomial of* α *through its approximation* $\mod p^{1024}$ *using* LLL*:* 520 *sec.* □

For the detail of other examples, see http://math.unice.fr/∼cbertone/
In the following table we resume the timings of a few more examples.

- $n = \mathrm{tdeg}\,(f)$, s=number of absolute factors of f, $m = n/s$=degree of an absolute factor of f;
- p= prime integer, λ = level of accuracy of Proposition 1.4.11, $\tilde{\lambda}$ =chosen level of accuracy;
- T_1 = time to factor $f(X, Y) \mod p$, T_2 =time to lift the factorization to $p^{\tilde{\lambda}}$, T_3 =time to find the minimal polynomial of α.

Example	n	s	m	p	λ	$\tilde{\lambda}$	T_1	T_2	T_3
Example 1.1	50	5	10	11	338	256	0.13 s	0.07 s	0.22 s
Example 1.2	50	5	10	307	141	128	0.13 s	0.08 s	0.4 s
Example 2.1	100	10	10	7	1105	512	3.4 s	0.3 s	2.25 s
Example 2.2	100	10	10	655379	160	128	6.2	0.4 s	5.7 s
Example 3.1	150	15	10	7	2246	1024	10 s	1.08 s	21 s
Example 4.1	200	10	20	47	853	512	33 s	2.8 s	14 s
Example 4.2	200	10	20	114041	282	256	128 s	3.8 s	30 s
Example 5	200	20	10	7682833	457	256	68 s	3.8 s	220 s
Example 6.1	400	20	20	53259165137	398	256	1924 s	39 s	1024 s
Example 6.2	400	20	20	127	2194	1024	127 s	24 s	520 s
Example 7	100	20	5	7	3029	2048	0.64 s	1.25 s	205 s

Chapter 2

Decomposition of curves in the 3-dimensional space

After the investigations of Chapter 1 concerning the decomposition of an algebraic curve in $\mathbb{C}^2$, we now face the problem of decomposing an algebraic curve of $\mathbb{C}^3$. We would like in this chapter to make clear what we are looking for. The geometric setting of our problem is quite simple:

> Given (through polynomial equations) an algebraic curve $\mathscr{C}$ of $\mathbb{C}^3$, we look for its irreducible components $\mathscr{C}_1, \ldots, \mathscr{C}_m$:
>
> $$\mathscr{C} = \mathscr{C}_1 \cup \cdots \cup \mathscr{C}_m.$$
>
> We will consider the case were *all* the $\mathscr{C}_i$'s are curves (not points).

From the algebraic viewpoint, the problem is the following:
we deal with an ideal $\mathfrak{a}$ in the polynomial ring $\mathbb{Q}[X, Y, Z]$; $\dim R/\mathfrak{a} = 1$ (see Definition 2.1.12) and $\mathfrak{a}$ has pure dimension 1 (see Definition 2.2.1). The ideal $\mathfrak{a}$ is not assumed to be prime nor radical, and we would like to find the equations defining the irreducible components of the curve $\mathscr{C} = V(\mathfrak{a})$.

It is well-known that the algebraic equivalent of this geometric decomposition is the computation of the primary decomposition of an ideal. Nevertheless, for lack of a complete reference, we prefer to recall the main definitions and properties and to establish explicitly the connection between the geometric viewpoint and the algebraic one. For the algebraic part, a very precise reference is [2], Chapter 4.

2.1 Primary Decomposition and Affine Hilbert function

Definition 2.1.1. *A proper ideal* $\mathfrak{q}$ *in a ring* R *is* primary *if the following condition holds:*

$$xy \in \mathfrak{q} \text{ and } x \notin \mathfrak{q} \Rightarrow y \in \sqrt{\mathfrak{q}}.$$

An ideal $\mathfrak{q}$ is primary if and only if $R/\mathfrak{q} \neq 0$ and all its zero divisors are nilpotent. Every prime ideal is obviously primary.

Proposition 2.1.2 ([2], Proposition 4.1)**.** *Let* $\mathfrak{q}$ *be a primary ideal in* R*. Then* $\mathfrak{p} = \sqrt{\mathfrak{q}}$ *is the smallest prime ideal containing* $\mathfrak{q}$*; we say that* $\mathfrak{q}$ *is* $\mathfrak{p}$*-primary.*

Definition 2.1.3. *A* primary decomposition *of an ideal* $\mathfrak{a}$ *in* R *is an expression of* $\mathfrak{a}$ *as a finite intersection of primary ideals:*

$$\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{q}_i. \tag{2.1.1}$$

If moreover

1. $\mathfrak{q}_i \not\supseteq \bigcap_{i \neq j} \mathfrak{q}_j$*;*
2. *the prime ideals* $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$ *are all distinct,*

then the primary decomposition (2.1.1) is said to be minimal *(or irredundant, or reduced, or normal). Any primary decomposition can be reduced to a minimal one (see [2], page 52).*

Remark 2.1.4. *In general, a primary decomposition may not exist, this is why in the general theory of primary decomposition we may sometimes need to assume that an ideal is decomposable. Actually, this is not the case if we work with a polynomial ring: in this case all ideals have a primary decomposition (Lasker-Noether Decomposition Theorem).*

Theorem 2.1.5 ([2], Theorem 4.5.)**.** *Let* $\mathfrak{a}$ *be a decomposable ideal and let* $\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{q}_i$ *be a minimal primary decomposition of* $\mathfrak{a}$*. Let* $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$ *(*$1 \leq i \leq n$*). Then the* $\mathfrak{p}_i$*'s are independent of the particular decomposition of* $\mathfrak{a}$*.*

In practice, a primary decomposition is the algebraic equivalent of the geometric decomposition of a variety: but a primary decomposition carries (like the factorization of a polynomial) many information, such as the degree of the different components of the algebraic variety defined by $\mathfrak{a}$, their multiplicities and also the *embedded components* of $\mathfrak{a}$ (for the exact definition degree and multiplicity, see Definitions 2.1.14 and 2.1.15).

Example 2.1.6. *Consider the ideal* $\mathfrak{a} = (X^2, XY)$ *in* $R = \mathbb{K}[X, Y]$*. A minimal primary decomposition is* $\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2$*, where* $\mathfrak{q}_1 = (X)$*,* $\mathfrak{q}_2 = (X, X^2Y)$ *and* $\sqrt{\mathfrak{q}_2} = \mathfrak{p}_2 = (X, Y)$*. The ideal* $\mathfrak{q}_1$ *is prime, so* $\sqrt{\mathfrak{q}_1} = \mathfrak{p}_1$*. So the prime ideals associated to* $\mathfrak{a}$ *are* $\mathfrak{p}_1, \mathfrak{p}_2$*. Furthermore, observe that* $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$*; we have* $\sqrt{\mathfrak{a}} = \mathfrak{p}_1 \cap \mathfrak{p}_2 = \mathfrak{p}_1$*, but* $\mathfrak{a}$ *is not a primary ideal.*

The prime ideals $\mathfrak{p}_i$ in Theorem 2.1.5 are said to belong to $\mathfrak{a}$, or to be *associated* with $\mathfrak{a}$. The minimal elements of the set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ are called the *minimal* or *isolated* prime ideals belonging to $\mathfrak{a}$. The others are called *embedded* prime ideals. In the example above, $\mathfrak{p}_2 = (X, Y)$ is embedded.

The names "isolated" and "embedded" come from geometry. The ideal $\mathfrak{a}$ gives rise to a variety $W \subseteq \mathbb{K}^n$. The minimal primes $\mathfrak{p}_i$ correspond to the irreducible components of W which are not included in other ones and the embedded primes correspond to subvarieties of these, i.e., components embedded in the subvarieties defined by the minimal primes. Thus in Example 2.1.6 the variety defined by $\mathfrak{a}$ is the line $X = 0$ and the embedded prime ideal $\mathfrak{p} = (X, Y)$ corresponds to the origin $(0, 0)$.

A set Σ of prime ideals belonging to $\mathfrak{a}$ is said to be *isolated* if it satisfies the following condition: if $\mathfrak{p}'$ is a prime ideal belonging to $\mathfrak{a}$ and $\mathfrak{p}' \subseteq \mathfrak{p}$ for some $\mathfrak{p} \in \Sigma$, then $\mathfrak{p}' \in \Sigma$.

Theorem 2.1.7 ([2], Theorem 4.10)**.** *Let $\mathfrak{a}$ be a decomposable ideal, let $\mathfrak{a} = \bigcap \mathfrak{q}_i$ be a minimal primary decomposition of $\mathfrak{a}$, and let $\{\mathfrak{p}_{i_1}, \ldots, \mathfrak{p}_{i_m}\}$ be an isolated set of prime ideals of $\mathfrak{a}$. Then $\mathfrak{q}_{i_1} \cap \cdots \cap \mathfrak{q}_{i_m}$ is independent of the decomposition.*

Corollary 2.1.8. *The isolated primary components of $\mathfrak{a}$ (i.e., the primary components $\mathfrak{q}_i$ corresponding the minimal prime ideals $\mathfrak{p}_i$) are uniquely determined by $\mathfrak{a}$.*

On the contrary, the embedded primary components (i.e., the primary components corresponding to embedded primes) are not unique.

Example 2.1.9. *Consider the ideal $\mathfrak{a}$ of Example 2.1.6. The primary decomposition $\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2$ is not the unique one; we also have $\mathfrak{a} = (X) \cap (X^2, X + Y)$, which is a minimal primary decomposition too. Remark that the associated primes are the same, but the embedded primary component changes.*

Considering the parallelism between the factorization of $f(X, Y) \in \mathbb{Q}[X, Y]$ in $\mathbb{C}[X, Y]$, and the primary decomposition of an ideal $\mathfrak{a} \subseteq \mathbb{Q}[X, Y, Z]$ in $\mathbb{C}[X, Y, Z]$, it is natural to talk about *degree* and *multiplicity* of a component. We can define them through the Affine Hilbert function.

Definition 2.1.10. *Let $\mathbb{K}$ be a field and $\mathfrak{a}$ an ideal of the polynomial ring $R = \mathbb{K}[X_1, \ldots, X_n]$ standard graded.*

We first define $\langle R_{\leq i} \rangle$, the vector space generated by all the polynomials of R of degree $\leq i$. The $\mathbb{K}$-vector space $\langle \mathfrak{a}_{\leq i} \rangle$ is the vector subspace of $\langle R_{i \leq i} \rangle$ which consists of the polynomials of $\mathfrak{a}$ of degree $\leq i$. Since $\mathfrak{a}_{\leq i} = R_{\leq i} \cap \mathfrak{a}$, we can view the vector space $R_{\leq i}/\mathfrak{a}_{\leq i}$ as a vector subspace of $R/\mathfrak{a}$. In the following we shall frequently use this identification.

The map $HF^a_{R/\mathfrak{a}} : \mathbb{Z} \to \mathbb{Z}$ defined by

$$HF^a_{R/\mathfrak{a}}(i) = \dim_{\mathbb{K}}(\langle R_{\leq i} \rangle / \langle \mathfrak{a}_{\leq i} \rangle)$$

for $i \in \mathbb{Z}$ is called the affine Hilbert function *of $R/\mathfrak{a}$.*

Definition 2.1.11. *The power series $HS^a_{R/\mathfrak{a}}(z) = \sum_{i\geq 0} HF^a_{R/\mathfrak{a}}(i)z^i \in \mathbb{Z}[[z]]$ is called the* affine Hilbert series *of $R/\mathfrak{a}$.*

The affine Hilbert series of $R/\mathfrak{a}$ is of the form

$$HS^a_{R/\mathfrak{a}}(z) = \frac{HN^a_{R/\mathfrak{a}}(z)}{(1-z)^{n+1}},$$

with a polynomial $HN^a_{R/\mathfrak{a}}(z) \in \mathbb{Z}[z]$ which is called the *affine Hilbert numerator* of $R/\mathfrak{a}$ (see [49],Part b) of Proposition 5.6.7 and Theorem 5.2.20).

We can simplify this fraction by cancelling $(1-z)$ as often as possible and obtain a representation $HS^a_{R/\mathfrak{a}}(z) = \frac{hn^a_{R/\mathfrak{a}}(z)}{(1-z)^{h+1}}$ with a polynomial $hn^a_{R/\mathfrak{a}}(z) \in \mathbb{Z}[z]$ and $0 \leq h \leq n$.

Definition 2.1.12. *Let $\mathfrak{a}$ be a proper ideal in R, and let $HS^a_{R/\mathfrak{a}}(z) = \frac{hn^a_{R/\mathfrak{a}}(z)}{(1-z)^{h+1}}$ be the simplified Hilbert series of $R/\mathfrak{a}$.*
The number $\dim(R/\mathfrak{a}) := h$ is called the dimension *of $R/\mathfrak{a}$.*

Definition 2.1.13. *Let $\mathfrak{a}$ be a proper ideal in R.*

1. *The uniquely determined integer valued polynomial $HP^a_{R/\mathfrak{a}}(t) \in \mathbb{Q}[t]$ such that*

$$HP^a_{R/\mathfrak{a}}(i) = HF^a_{R/\mathfrak{a}}(i) \text{ for all integers } i >> 0$$

   is called the affine Hilbert polynomial *of $R/\mathfrak{a}$.*

2. *The* affine regularity index *index of $R/\mathfrak{a}$ is*

$$\rho(R/\mathfrak{a}) = \min\{i \in \mathbb{Z} | HF^a_{R/\mathfrak{a}}(j) = HP^a_{R/\mathfrak{a}}(j) \text{ for all } j \geq i\}.$$

Definition 2.1.14. *Let $\mathfrak{a}$ be a proper ideal in R, consider its affine Hilbert polynomial $HP^a_{R/\mathfrak{a}}(t) \in \mathbb{Q}[t]$. The degree of $R/\mathfrak{a}$ is $(\dim(R/\mathfrak{a})!) \cdot (lcoeff(HP^a_{R/\mathfrak{a}}(t))$.*

We will often use some abuse of notations, writing $\dim \mathfrak{a}$ for $\dim(R/\mathfrak{a})$ or we will often say "the degree of $\mathfrak{a}$" meaning the degree of $R/\mathfrak{a}$.

Finally, once defined the degree of an ideal, we can define the multiplicity of a primary component. Here we state the proper algebraic definition, but it corresponds to the intuitive idea that the multiplicity is "how many times the component should be counted".

Definition 2.1.15. *Let $\mathfrak{q} \in R$ be a $\mathfrak{p}$-primary ideal. Then the* multiplicity *of $\mathfrak{q}$ in $\mathfrak{p}$ is* $\deg(\mathfrak{p})/\deg(\mathfrak{q})$.

2.2 Setting of the problem and main aim

After the general definitions and properties of primary decomposition of the previous section, we now state the precise hypothesis in which we want to work and the main aim of an algorithm of decomposition of a curve.

Definition 2.2.1. *An ideal* $\mathfrak{a}$ *has* pure dimension 1 *if all its associated primes* $\mathfrak{p}_i$ *have dimension 1.*

In other words, if an ideal $\mathfrak{a}$ has pure dimension 1, then there are no embedded primes. Thanks to Corollary 2.1.8, all the primary components of $\mathfrak{a}$ are uniquely determined and so in this case the primary decomposition is unique.

If we consider a complete intersection curve $\mathscr{C}$, defined by the ideal $\mathfrak{a} = (F, G) \in \mathbb{Q}[X, Y, Z]$, then $\mathscr{C}$ has pure dimension 1. This can be seen as a consequence of the Affine Dimension Theorem ([40], Chapter II, Proposition 7.1).

Definition 2.2.2. *Consider* $\mathfrak{a} = (F, G) \subseteq \mathbb{Q}[X, Y, Z]$.

We say that the minimal primary decomposition of $\mathfrak{a}$ *in* $\mathbb{Q}[X, Y, Z]$

$$\mathfrak{a} = \bigcap_{j=1}^{s} \mathfrak{q}_i, \mathfrak{q}_i \in \mathbb{Q}[X, Y, Z]$$

is the rational primary decomposition *of* $\mathfrak{a}$.
Furthermore, we consider the primary decomposition of each primary component $\mathfrak{q}_i$ *in* $\mathbb{C}[X, Y, Z]$*:*

$$\mathfrak{q}_i = \bigcap_{j=1}^{r_i} \mathfrak{q}_i^{(j)} \subseteq \mathbb{C}[X, Y, Z].$$

We say that $\mathfrak{q}_i$ *(resp.* $V(\mathfrak{q}_i)$*) is a* rational component *of* $\mathfrak{a}$ *(resp. of* $V(\mathfrak{a})$*). If* $r_i = 1$*, we say that* $\mathfrak{q}_i$ *(resp.* $V(\mathfrak{q}_i)$*) is* purely rational.

Consider a non-purely rational component $\mathfrak{q}_i$ of $\mathfrak{a}$. Let $\mathbb{L}_i$ be the smallest normal algebraic extension of $\mathbb{Q}$ such that $\mathfrak{q}_i^{(1)}$ has a set of generators in $\mathbb{L}_i[X, Y, Z]$. Consider the Galois group of $\mathbb{L}_i$ over $\mathbb{Q}$, $Gal(\mathbb{L}_i/\mathbb{Q})$.

For every $\sigma \in Gal(\mathbb{L}_i/\mathbb{Q})$, starting from $\mathfrak{q}_i^{(1)}$, with $\sqrt{\mathfrak{q}_i^{(1)}} = \mathfrak{p}_i^{(1)}$, we can define an ideal in the following way

$$\mathfrak{q}_i^{(1)} = (f_1(\alpha_i, X, Y, Z), \ldots, f_l(\alpha_i, X, Y, Z)) \rightarrow \\ \rightarrow \sigma(\mathfrak{q}_i^{(1)}) = (f_1(\sigma(\alpha_i), X, Y, Z), \ldots, f_l(\sigma(\alpha_i), X, Y, Z)).$$

Obviously, the definition of $\sigma(\mathfrak{q}_i^{(1)})$ is independent from the chosen set of generators of $\mathfrak{q}_i^{(1)}$, $\mathfrak{q}_i^{(1)}$ and $\sigma(\mathfrak{q}_i^{(1)})$ have the same dimension and it is straightforward that the ideal $\sigma(\mathfrak{q}_i^{(1)})$ is

$\sigma(\mathfrak{p}_i^{(1)})$-primary. Finally, if $\tau, \sigma \in Gal(\mathbb{L}_i/\mathbb{Q})$, $\tau \neq \sigma$, then $\tau(\mathfrak{q}_i^{(1)}) \neq \sigma(\mathfrak{q}_i^{(1)})$ and $\tau(\mathfrak{p}_i^{(1)}) \neq \sigma(\mathfrak{p}_i^{(1)})$.
We now show that actually the ideals $\sigma(\mathfrak{q}_i^{(1)})$ are the primary components of $\mathfrak{q}_i$ in $\overline{\mathbb{Q}}[X, Y, Z]$.

Lemma 2.2.3. *With the previously used notations, consider $\mathfrak{q}_i$ a non-purely rational component of $\mathfrak{a} = (F, G)$, $\mathbb{L}_i$ the smallest normal algebraic extension of $\mathbb{Q}$ such that $\mathfrak{q}_i^{(1)}$ has a set of generators in $\mathbb{L}_i[X, Y, Z]$, $Gal = Gal(\mathbb{L}_i/\mathbb{Q})$. The minimal primary decomposition of $\mathfrak{q}_i$ is*

$$\mathfrak{q}_i = \bigcap_{\sigma \in Gal} \sigma\left(\mathfrak{q}_i^{(1)}\right), \tag{2.2.1}$$

and in particular $r_i = [\mathbb{L}_i : \mathbb{Q}]$.

Proof. $\sigma(\mathfrak{q}_{ij})$ is $\sigma(\mathfrak{p}_{ij})$-primary. So $\bigcap_{\sigma \in Gal} \sigma\left(\mathfrak{q}_i^{(1)}\right)$ is a primary decomposition of an ideal $\mathfrak{b}$.

Furthermore, it is a minimal primary decomposition. Thanks to the definition of the ideals through the automorphism of $\mathbb{L}_i$, all the associated primes $\sigma_i(p_i^{(1)})$ are distinct; for what concerns redundant primary components, for any $\sigma \in Gal$, since $\mathbb{L}_i$ is the minimal normal algebraic extension containing a set of generators of $\mathfrak{q}_i^{(1)}$, then there is $f \in \mathfrak{q}_i^{(1)}$ such that $\prod_{\tau \neq \sigma} \tau(f)$ is not in $\sigma(\mathfrak{q}_i^{(1)})$.

We now consider the associated primes of $\mathfrak{q}_i$ in the decomposition over $\mathbb{L}_i[X, Y, Z]$ and the natural homomorphism $\mathbb{Q}[X, Y, Z] \to \mathbb{L}_i[X, Y, Z]$. We can apply [2], Exercise 13 of Chapter 5: the set of prime ideals $\{\mathfrak{p}_i^{(j)}\}$ is the same as the set of prime ideals of $\mathbb{L}_i[X, Y, Z]$ whose contraction is $\mathfrak{p}_i$. Then Gal acts transitively on the set $\{p_i^{(j)}\}_{j=1,\dots,r_i}$, that is

$$\{p_i^{(j)}\}_{j=1,\dots,r_i} = \{\sigma(\mathfrak{p}_i^{(1)})\}_{\sigma \in Gal}.$$

So $\bigcap_{\sigma \in Gal} \sigma\left(\mathfrak{q}_i^{(1)}\right)$ is a minimal primary decomposition of $\mathfrak{q}_i$; since $\mathfrak{q}_i$ is a primary component of dimension 1 of the complete intersection $\mathfrak{a}$, all its primary components in $\mathbb{L}_i[X, Y, Z]$ are of dimension 1 and there are no embedded components, so thanks to Corollary 2.1.8, we have that this decomposition is the unique one. □

Lemma 2.2.4. *Consider $\mathfrak{a} = (F, G) \subseteq \mathbb{Q}[X, Y, Z]$. Then the minimal primary decomposition of $\mathfrak{a}$ is*

$$\mathfrak{a} = \bigcap_{i=1}^{r} \left(\bigcap_{\sigma \in Gal(\mathbb{L}_i/\mathbb{Q})} \sigma\left(q_i^{(1)}\right) \right). \tag{2.2.2}$$

Proof. Since all of this ideals are primary, we just need to show that the decomposition is minimal.

Condition 1 of Definition 2.1.3 about minimality is straightforward from Lemma 2.2.3.

For what concerns Condition 2, we just have to point out that if there is $\tilde{\mathfrak{p}}$ associated to $\mathfrak{q}_i$ and $\mathfrak{q}_j$, $i \neq j$, then thanks to the choice of the extensions, we have $\mathbb{L}_i = \mathbb{L}_j$ and so $\mathfrak{p}_i = \mathfrak{p}_j$. But this contradicts the minimality of the rational primary decomposition of $\mathfrak{a}$. □

Up to relabelling the automorphisms of $Gal(\mathbb{L}_i/\mathbb{Q})$, we can rewrite (2.2.2) as

$$\mathfrak{a} = \bigcap_{i=1}^{r} \left(\bigcap_{j=1}^{r_i} \mathfrak{q}_i^{(j)} \right), \tag{2.2.3}$$

with $r_i = [\mathbb{L}_i : \mathbb{Q}]$, $\mathfrak{q}_i^{(j)} = \sigma_j \left(\mathfrak{q}_i^{(1)} \right)$.

Definition 2.2.5. *Writing the primary decomposition of* $\mathfrak{a}$ *as in (2.2.3), for* i *such that* $r_i \geq 2$*, we say that* $\mathfrak{q}_i^{(j)}$ *(resp.* $V(\mathfrak{q}_i^{(j)})$*) is an* algebraic component *of* $\mathfrak{a}$ *(resp. of* $V(\mathfrak{a})$*).*

We can finally fix our purpose.

Given a non-prime ideal $\mathfrak{a} = (F, G) \subseteq \mathbb{Q}[X, Y, Z]$, we write its primary decomposition as in (2.2.3). Then, there are polynomials

$$Q_i^{(j)} \in \mathbb{L}_i[X, Y, Z], i = 1, \ldots, s, j = 1, \ldots, r_i, \text{ and } P \in \mathbb{Q}[X, Y, Z]$$

such that

- $\mathbb{L}_i$ minimal normal algebraic extension containing $\mathfrak{q}_i^{(1)}, r_i = [\mathbb{L}_i : \mathbb{Q}]$,
- $Q_i^{(j)} \in \mathfrak{q}_i^{(j)}, Q_i^{(j)} \notin \mathfrak{a}$,
- $Q_i^{(j)} = \sigma(Q_i^{(1)})$ for some $\sigma \in Gal(\mathbb{L}_i/\mathbb{Q})$,
- $Q_i^{(j)} \notin \mathfrak{q}_m^{(l)} \forall (i, j) \neq (m, l)$,
- $P = \prod_{i=1}^{s} \left(\prod_{j=1}^{r_i} Q_i^{(j)} \right) \in \mathfrak{a}$.

We then would like to find
for every primary component of $\mathfrak{a}$, its degree and multiplicity (with respect to the associated prime)
for i from 1 to s, a polynomial $M_i(T) \in \mathbb{Q}[T]$, monic, $\deg M_i(T) = [\mathbb{L}_i : \mathbb{Q}]$, such that $\mathbb{L}_i \simeq \mathbb{Q}[T]/M_i(T)$ and a polynomial $Q_i \in \mathbb{Q}[X, Y, Z]$ such that

$$Q_i = \prod_{j=1}^{r_i} Q_i^{(j)}$$

where $Q_i^{(1)} \in \mathfrak{q}_i^{(1)} \subseteq \mathbb{Q}(\alpha_i)[X, Y, Z]$, $Q_i^{(j)} = \sigma_j(Q_i^{(j)})$.

Definition 2.2.6. *With the above notations, we say that* Q_i *(resp.* $Q_i^{(j)}$*) is a* separator polynomial *for the rational component* $\mathfrak{q}_i$ *(resp. for the algebraic component* $\mathfrak{q}_i^{(j)}$*) of* $\mathfrak{a}$*.*

2.3 Related works

The aim for a decomposition algorithm for curves we established is actually the same that we can found in [29] and in [73] (and the related [72] and [74]). All of this algorithms are "numerical", in the sense that they use floating-point computation and not symbolic one.
There is an underlying common technique in this papers: considering a generic plane section of the curve $\mathscr{C}$, that is a finite set of points, one can get the degrees of the components and their multiplicity. More precisely, in order to obtain the degrees and multiplicities of all the algebraic components of $\mathscr{C}$, in [29] there is a zero-sum criterion, which generalizes the strategy of [68] for absolute factorization, while in [73], the points of the generic plane section are divided according to the decomposition of the curve in irreducible components using homotopy continuation methods.
Finally, in both approaches the authors construct a polynomial defining an hypersurface which can isolate a component from the others (in our language, a separator polynomial). In both cases, since the knowledge of the generic plane section of a component is not enough to construct a separator polynomial (see Section 3.2), the authors "move" the plane they used to cut the variety in order to get more points and conditions on the separator polynomial. The result is a polynomial of degree equal to the degree of the component itself.
Beyond the limits of these algorithms concerning the degrees of the considered curves and the needed precision to have correct outputs, we also point out a particular aspect that we wish to improve: the degree of the separator polynomial found through the techniques in [29] and [73] is the degree of the associated component; actually, we would like to find a separator polynomial with a lower degree, or at least a bound on this degree better than the degree of the component itself, using for instance the Hilbert function of the component.

There is another group of papers ([51] and the references therein) using a more symbolic approach to the problem. Instead of using the plane sections, the authors use lifting fibers, that is the input and output of a decomposition algorithm are encoded in a computationally efficient way, that is straight-line programs (see [33]).

Chapter 3

Bounds on the degree

We consider an ideal $\mathfrak{a} \subseteq \mathbb{Q}[X, Y, Z]$ complete intersection: $\mathfrak{a} = (F, G)$ with $\deg F = d_1$ and $\deg G = d_2$.

We would like to find a bound on the degree of a separator polynomial for each irreducible component of $\mathscr{C}$.

In the next sections, we will sometimes pass to consider a curve $\mathscr{C}$ of the affine N-dimensional space $\mathbb{C}^N$ as a curve of the projective space $\mathbb{P}^N$. This means that if the ideal $\mathfrak{a} \subseteq \mathbb{C}[X_1, \ldots, X_N]$ defines $\mathscr{C}$ in the sense that $V(\mathfrak{a}) = \mathscr{C}$, we can consider the curve $\mathscr{C}$ in $\mathbb{P}^N$ homogenizing a set of generators of $\mathfrak{a}$ with a new variable X_0 and then saturating the obtained ideal with respect to X_0 (see [49], Proposition 4.3.5). If we use a term ordering on the variables, we always assume that the homogenizing variable is the smallest one. If we consider the polynomial ring $\mathbb{K}[X, Y, Z]$, we denote the homogenizing variable with W. From now on, with R we mean the polynomial ring $\mathbb{K}[X_1, \ldots, X_N]$ or $\mathbb{K}[X, Y, Z]$ ($\mathbb{K} = \mathbb{C}$ or $\mathbb{Q}$), and with $\overline{R}$ we mean the polynomial ring $R[X_0]$ or $R[W]$.

When we use the language of sheaves and cohomology, we refer to [40] for definitions and properties.

For computational purposes, we always assume that we performed a generic change of coordinates in the following way: we consider the homogenized ideal $\mathfrak{a}$ in $\overline{R}$ and perform a generic linear change of coordinates. If needed, we go back to the affine space substituting 1 to the homogenizing variable. In this way we avoid problems with irreducible components at infinity of the curve.

3.1 Guide-line example

We consider an explicit example of an ideal $\mathfrak{a} \subseteq \mathbb{Q}[X, Y, Z]$ defining a complete intersection curve $\mathscr{C}$ of $\mathbb{C}^3$ with two irreducible components. This example is quite simple, since in this case all the components are purely rational.

Example 3.1.1. *We consider the complete intersection* $\mathfrak{a} = (F, G) \subseteq \mathbb{Q}[X, Y, Z]$ *with*

$$F(X, Y, Z) = X^3 + 2\,X^2Z + 3\,XYZ - 16\,X^2Y - 48\,Y^2X - 36\,Y^3,$$

$$G(X, Y, Z) = 5\,X^2Z + 64\,X^2Y + 96\,Y^2X + 16\,X^3 + 12\,XYZ + 9\,Y^2Z + 54\,Y^3.$$

The primary decomposition of $\mathfrak{a}$ *is*

$$\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2,$$

with $\mathfrak{q}_1$ *prime,* $\mathscr{C}_1 = V(\mathfrak{q}_1)$ *reduced curve of degree 5,* $\sqrt{\mathfrak{q}_2} = (X, Y)$ *so* $V(\mathfrak{q}_2)$ *is a line, with multiplicity 4.*

3.2 The Lifting Problem

The simpler idea one can think of in order to find separator polynomials is getting information from the generic plane section of the curve:
if $\mathfrak{a} \in \mathbb{C}[X, Y, Z]$, we can consider a generic plane $H \in \mathbb{C}^3$ defined by the equation $h \in \mathbb{C}[X, Y, Z]$ and consider the ideal $\mathfrak{a} + (h)$, which corresponds to the intersection of the curve $\mathscr{C}$ with the plane H. This is actually the starting point of the Algorithms described in [73] and [29]. Actually, both these algorithms use some information further than the generic plane section of the curve (for instance the Taylor expansion to a given degree of the curve around a point of the section); we may say that they use some "fat" plane section. Usually the degree of the Taylor expansion used (and of the separator polynomial constructed) is the degree of the curve itself. It is interesting to find a better (lower) bound on the degree of a separator polynomial.

The datas we have to find a separator polynomial (or at least its degree) are at the moment

- $F, G \in \mathbb{Q}[X, Y, Z]$;
- the sets of points $\mathscr{C}_i \cap H$, H general hyperplane, with $\#\{\mathscr{C}_i \cap H\} = \deg \mathscr{C}_i$.

Given $\mathfrak{a} \subseteq \mathbb{Q}[X, Y, Z]$ such that $V(\mathfrak{a}) = \mathscr{C}$ curve of $\mathbb{C}^3$, we can consider a generic plane H and compute the points in $V(\mathfrak{a} + (h))$, with $V(h) = H$.

Assume that we are able to compute a partition of the set of points $V(\mathfrak{a}+(h)) = \mathscr{C} \cap H = \{p_j\}_{j \in J}$ such that:

$$\mathscr{C}_i \cap H = P_i = \{p_{ij}\}_{j=1,\dots,\deg \mathscr{C}_i}.$$

We can for instance, use the method of [29].

For each i, we can find a minimal non negative integer t_i such that

$$\binom{t_i + 2}{2} - 1 > \deg \mathscr{C}_i \tag{3.2.1}$$

Then we can find a curve lying on the plane H which interpolates the points of $\mathscr{C}_i \cap H$. If the points are not in general position, then the minimal degree for a curve of H containing $\{\mathscr{C}_i \cap H\}$ may be smaller than the t_i of equation (3.2.1).

Once that we have found the equation of such a curve, $Q_i^{(0)}$, we may think that we should just "lift" this curve to a surface of the same degree containing the whole curve $\mathscr{C}_i$. Beyond the problems of interpolation about this lifting, there are irreducible curves such that the minimal degree containing the general plane section is smaller than the minimal degree of a surface containing the curve. In literature this is a classical problem, the *Lifting Problem*.

Its precise statement, for varieties of codimension 2 in the projective space of dimension N is as follows:

> Let X be a nondegenerate reduced and irreducible variety of codimension 2 and degree d in $\mathbb{P}^N$ and Y be its generic hyperplane section. The *lifting problem* consists in finding numerical conditions involving d, N and a positive integer t, implying that any (or at least one) hypersurface of H of degree t containing Y can be lifted to a hypersurface of degree t containing X.

We point out the cohomological aspect of this lifting problem. It is interesting because the cohomology groups we will now look at will be found again in the next section.
The key point of the problem is that if we consider the curve $\mathscr{C}_i$ in the projective space $\mathbb{P}^3$ and we consider the sheafification $\mathcal{I}_{\mathscr{C}_i}$ of the homogeneous ideal of $\mathscr{C}_i$ in $\mathbb{P}^3$ we have the exact sequences

$$0 \to \mathcal{I}_{\mathscr{C}_i}(t-1) \to \mathcal{I}_{\mathscr{C}_i}(t) \to \mathcal{I}_{\mathscr{C}_i \cap H}(t) \to 0$$

$$0 \to H^0\mathcal{I}_{\mathscr{C}_i}(t-1) \to H^0\mathcal{I}_{\mathscr{C}_i}(t) \to H^0\mathcal{I}_{\mathscr{C}_i \cap H}(t) \to H^1\mathcal{I}_{\mathscr{C}_i}(t-1) \to H^1\mathcal{I}_{\mathscr{C}_i}(t)$$

If a degenerate curve of H of degree t contains $\mathscr{C}_i \cap H$ but no surfaces of $\mathbb{P}^3$ of degree t contain $\mathscr{C}_i$, then the map $H^0\mathcal{I}_{\mathscr{C}_i}(t) \to H^0\mathcal{I}_{\mathscr{C}_i \cap H}(t)$ is not surjective or, in other words, the map $H^1\mathcal{I}_{\mathscr{C}_i}(t-1) \to H^1\mathcal{I}_{\mathscr{C}_i}(t)$ has a non trivial kernel. We will see later that this problem, using language of sheaves and cohomology, will keep on troubling us in the search for a bound on the degree on the separator polynomial.

At the moment there is no a numerical general condition ensuring the lifting of the hyperplane section which work for any N, but there is a conjecture proposed by Mezzetti in [56]:

Conjecture 3.2.1. *If* $d > t^2-(N-3)t+\binom{N-2}{2}+1$ *then* X *is contained in a hypersurface of degree* t.

This conjecture is true for "small" values of N, but almost nothing is known about higher N's without adding some hypothesis on X. Here we list some of the main results.

For $N = 3$, that is for curves in $\mathbb{P}^3$, the conjecture is proved by Laudal's generalized trisecant lemma ([50]), in which the author obtained a first weaker bound $d > t^2 + t$. This bound was later improved by Gruson and Peskine ([38]) and Strano ([76]), with two different methods, getting the better bound $d > t^2 + 1$.
For $N = 4$, the bound $d > t^2 - t + 2$ is proved by Mezzetti in [56] in the general setting, but with some further hypothesis the bound was already proved by Mezzetti and Raspanti in [57].
For $N = 5$, the bound $d > t^2 - 2t + 4$ is proved by Valenzano in [80] in the general setting, while for the case $t > 5$ it was already proved by Mezzetti in [56].
For $N = 6$, the bound $d > t^2 - 3t + 7$ is proved by Roggero in [67].
For $N = 7$, the bound $d > t^2 - 4t + 11$ is not yet proved in the general case; with a further assumption on a cohomology group of X, it is proved by Roggero in [67].
For any N, the conjecture is proved by Roggero in [67] using an additional hypothesis on the vanishing of a cohomology group of the *plane* section of X, improving the results by Tortora in [77].

Example 3.2.2. *If we consider the curve $\mathscr{C}_1$ of degree 5 of Section 3.1.1 as a curve in $\mathbb{P}^3$, the plane section $\mathscr{C}_1 \cap H$ is made up of 5 points, which lie on a conic curve of H, but the sufficient condition $d > t^2 + 1$ in this case does not hold. Indeed, the curve $\mathscr{C}_1$ does not lie on a quadric surface of $\mathbb{P}^3$: the minimal free resolution of the ideal $\mathfrak{a}$ is*

$$0 \to R(-6) \to R^3(-4) \oplus R^2(-5) \to R^4(-3) \oplus R(-4) \to \mathfrak{a} \to 0.$$

Mezzetti's conjecture was inspired by Gruson and Peskine's proof of the bound for curves, [38].
Gruson and Peskine's method, in the general case of a codimension 2 subvariety X of $\mathbb{P}^N$, brings back the problem to the positivity of a Chern Class. Indeed, with the hypothesis that $H^0\mathcal{I}_X(t) = 0$ (that is X is not contained in any hypersurface of degree t), they define an injective morphism of sheaves from $\Omega_H(1)$ (the cotangent bundle of H shifted in degree) to $\mathcal{I}_\Delta(s)$ (with $\mathcal{I}_\Delta$ ideal sheaf of S, S hypersurface of H containing Y). The kernel of this map is a reflexive sheaf $\mathcal{N}$:

$$0 \to \mathcal{N} \to \Omega_H(1) \to \mathcal{I}_\Delta(t) \to 0.$$

The *second Chern class* of $\mathcal{N}(1)$ is $t^2 - (N-1)t + \binom{N}{2} + 1 - \delta$, where $\delta \geq d$ is the degree of the closed subscheme Δ of S. So the problem turns to finding hypothesis on a reflexive sheaf on $\mathbb{P}^N$ in order to have its second Chern class to be non-negative.

3.2.1 Positivity of Chern classes of reflexive sheaves

There are clear and complete results on the positivity of the Chern classes for what concerns vector bundles (see [27], Example 12.1.7). A reflexive sheaf is in some sense a "more gen-

eral" coherent sheaf than a vector bundle: a reflexive sheaf on $\mathbb{P}^N$ is a vector bundle except along a closed subset of $\mathbb{P}^N$ of codimension ≥ 3.

We studied the positivity of the Chern classes (in particular of the first and second one) of a reflexive sheaf $\mathcal{F}$ on $\mathbb{P}^N$ in [6] and [7], putting them in connection with some invariant sequences of integers of the sheaf.
In [6], after defining a injective morphism $\oplus_{i=1}^{n-1}\mathcal{O}_{\mathbb{P}^N}(a_i) \to \mathcal{F}$, for a maximal sequence $(a_1, \ldots, a_n)$ of integers, we are able to show, using induction on the rank of $\mathcal{F}$ and combinatorial properties on the number of global sections of the involved sheaves, the following bounds for the first and second Chern class $c_1(\mathcal{F})$ and $c_2(\mathcal{F})$ of $\mathcal{F}$:

> If $\mathcal{F}$ is not a direct sum of line bundles and it has a proper subsheaf isomorphic to $\oplus_{i=1}^{n}\mathcal{O}_{\mathbb{P}^N}(a_i)$ where $a_1 \geq \cdots \geq a_n \geq 0$, then:
>
> $$c_1(\mathcal{F}) \geq \sum_{i=1}^{n} a_i + 1 \text{ and } c_2(\mathcal{F}) \geq \sum_{i<j} a_i a_j + \sum_{i\neq 2} a_i + 1.$$
>
> Moreover
>
> $$c_1(\mathcal{F}) \geq \sum_{i=1}^{n} a_i + 2 \text{ and } c_2(\mathcal{F}) \geq \sum_{i<j} a_i a_j + \sum_{i\neq 2} a_i + 2,$$
>
> unless $\mathcal{F}$ has a short free resolution of the type:
>
> $$0 \to \mathcal{O}_{\mathbb{P}^N}(\beta - 1) \to \oplus_{i=1}^{n}\mathcal{O}_{\mathbb{P}^N}(a_i) \oplus \mathcal{O}_{\mathbb{P}^N}(\beta) \to \mathcal{F} \to 0,$$
>
> where β depends on $c_2(\mathcal{F})$ and the integers a_i.

Furthermore, some results about positivity of $c_1(\mathcal{F})$ and $c_2(\mathcal{F})$ are obtained using weaker hypotheses on the maximal sequence $(a_1, \ldots, a_n)$ but assuming that $\mathcal{F}$ has a particular splitting type. Finally, we also investigate $c_3(\mathcal{F})$, but there we need completely different techinques (for instance, hypotheses on the homological dimension of the sheaf and on the codimension of its singular locus).

In [7], instead of using the sequence $(a_1, \ldots, a_n)$ of a reflexive sheaves, we generalize the inequalities of [6] to torsion-free sheaves using the *splitting type* of the sheaf $\mathcal{F}$, which is a well-known invariant of a coherent sheaf (see [62]).

> Let $\mathcal{F}$ be a torsion free sheaf on $\mathbb{P}^N$ and $\mathrm{st}(\mathbb{F}) = (b_1, \ldots, b_n), b_1 \geq \cdots \geq b_n$, be its splitting type. Then
>
> $$c_2(\mathcal{F}) \geq c_2(\oplus\mathcal{O}_{\mathbb{P}^N}(b_i)).$$

Actually, the starting point for the above result is the inequality about the dimension of the 0-th cohomology group:

$$h^0(\mathcal{F}) \leq h^0(\oplus\mathcal{O}_{\mathbb{P}^N}(b_i)).$$

It is a classical technique (see [39], Theorem 2.3) to write the Euler characteristic of a coherent sheaf $\mathcal{F}$ (which involves the dimensions of the cohomology groups $h^i\mathcal{F}$) as a polynomial in the Chern classes of the sheaf itself. In [39] this is applied to a coherent sheaf of rank n on $\mathbb{P}^3$, but the technique can be extended to a sheaf of any rank on $\mathbb{P}^N$. We explicitly carried out the computation of this polynomial for $\chi(\mathcal{F})$ in [4].
Actually what we prove in [7] is something more precise than the simple positivity of the two differences $h^0(\oplus\mathcal{O}_{\mathbb{P}^N}(b_i)) - h^0\mathcal{F}$ and $c_2(\mathcal{F}) - c_2(\oplus\mathcal{O}_{\mathbb{P}^N}(b_i))$; in fact we obtain lower bounds for them that involve the maximal free subsheaves of $\mathcal{F}$ and of its restriction $\mathcal{F}_H$ to general linear subspaces H in $\mathbb{P}^N$.
Interesting consequences of these results are a generalization of Schwartzenberger's inequality for rank 2 semistable vector bundles and a simple, self-included proof of a splitting criterion for torsion-free sheaves, generalizing Horrock's splitting criterion.

3.3 A bound using regularity

If we consider the case of an ideal $\mathfrak{a} = (F, G) \in \mathbb{Q}[X, Y, Z]$, at the moment we know that the degree q_i of the separator polynomial Q_i is greater or equal to t_i, that is the minimal degree of a curve of the plane containing $\mathscr{C}_i \cap H$. Furthermore, if $\deg \mathscr{C}_i > t_i^2 + 1$, then $\mathscr{C}_i$ is contained in a surface of degree t_i, but if $\deg \mathscr{C}_i \leq t_i^2 + 1$, we need to upper bound the degree of a surface containing $\mathscr{C}_i$, possibly using $\deg F = d_1$ and $\deg G = d_2$.

If we assume that the separator polynomial we are looking for is a *minimal generator* of $\mathfrak{q}_i$ such that $\mathfrak{q}_i$ is a primary component of $\mathfrak{a}$ and $V(\mathfrak{q}_i) = \mathscr{C}_i$, then a rough way to bound the degrees of the minimal generators of an ideal is the *regularity*.

In order to deal with regularity of an ideal, in this section we will keep on writing $\mathfrak{a}$ for the homogenization of $\mathfrak{a}$ in the polynomial ring $\mathbb{C}[X, Y, Z, W]$ if there is no ambiguity.

Definition 3.3.1. *Let $\mathfrak{m} = (X, Y, Z, W)$ be the maximal ideal in $\mathbb{C}[X, Y, Z, W]$. For $\mathfrak{a}$ homogeneous ideal, we define the numbers*

$$a_i(\mathfrak{a}) := \max\{\mu | H^i_{\mathfrak{m}}(\mathfrak{a})_\mu \neq 0\},$$

$$b_i(\mathfrak{a}) := \max\{\mu | Tor^i_{\mathfrak{m}}(\mathfrak{a}, \mathbb{C})_\mu \neq 0\}.$$

With these notations, the Castelnuovo-Mumford regularity *has the two following equivalent definitions*

$$reg(M) = \max_i\{a_i(\mathfrak{a}) + i\} = \max_j\{b_j(\mathfrak{a}) - j\}.$$

As an alternative, we can consider the minimal free resolution of $\mathfrak{a}$

$$0 \to E_4 \to E_3 \to E_2 \to E_1 \to E_0 \to \mathfrak{a} \to 0$$

where $E_i = \oplus_{j=1}^{\beta_i} R(-c_{ij})$.

We then have a third definition for regularity of $\mathfrak{a}$

$$reg(\mathfrak{a}) = \max\{c_{ij} - i\}.$$

This last definition enlightens clearly why we should use regularity to bound the degree of a separator polynomial: the regularity bounds not only the degrees of the minimal generators of $\mathfrak{a}$, but also the degrees of the generators of the minimal syzygies of $\mathfrak{a}$. So if we are looking for a separator polynomial which is also a minimal generator of the ideal $\mathfrak{a}$, its degree is bounded by the regularity of the ideal.
We want to underline that, while the bounds given by the Lifting Problem concern only the case of curves when $N = 3$, the regularity obviously bounds the degree of a minimal generator of $\mathfrak{a}$, ideal of $\mathbb{K}[X_1, \ldots, X_n]$ such that $\dim \mathfrak{a} = 1$ (affine dimension).

Unluckily, the best bound on the regularity of the ideal $\mathfrak{a} = I(\mathscr{C})$ associated to a reduced, irreducible and non-degenerate curve $\mathscr{C}$ in $\mathbb{P}^3$ is

$$\operatorname{reg}(\mathfrak{a}) \leq \deg \mathscr{C} - 1.$$

This bound was originally proved by Castelnuovo for smooth curves in [10] and then for reduced curves by Gruson, Lazersfeld and Peskine [37].

Using the notations of Section2.2, at the moment we have that, if $\mathfrak{q}_i$ has multiplicity one in the primary decomposition (that is $\mathfrak{q}_i = \sqrt{\mathfrak{q}_i}$),

$$\deg Q_i = q_i \leq \deg \mathscr{C}_i - 1 = \#\{\mathscr{C}_i \cap H\} - 1, \tag{3.3.1}$$

with H general plane.

If we use for instance the zero-sums method of [29], we can actually compute this bound. But if we want to have a bound on the degrees q_i's before starting our computations, we have at the moment just

$$q_i \leq d_1 \cdot d_2 - 1. \tag{3.3.2}$$

Example 3.3.2. *For the curve $\mathscr{C}_1$ of Example 3.1.1, the bound (3.3.1) is sharp for what concerns the regularity of the ideal $I(\mathscr{C}_1)$; for our purposes, we point out that the regularity is a good way to bound the degree of a separator polynomial of $\mathscr{C}_1$ but actually we can hope to find better, since the minimal degree of a generator of $\mathscr{C}_1$ is $3 < \operatorname{reg}(I(\mathscr{C}_1))$.*

It may be interesting to underline the role of $H^1\mathcal{I}_{\mathscr{C}_i}$, which is similar to the one pointed out for the Lifting Problem.

In [58], Mumford shows that Castelnuovo's results in [10] have other powerful consequences, starting from the definition of Castelnuovo-Mumford regularity for sheaves:

Definition 3.3.3. *A coherent sheaf $\mathcal{F}$ on $\mathbb{P}^N$ is* m-regular *if $H^i(m-i)=0$ for $i=0,\dots,N$. The minimal m for which $\mathcal{F}$ is m-regular its the* regularity *of the sheaf.*

For our purposes, one of the most interesting properties concerning regularity of sheaves is the following:

> Let $\mathcal{I}$ be an ideal sheaf in $\mathbb{P}^N$ and H a general hyperplane. $\mathcal{I}_H := \mathcal{I} \otimes \mathcal{O}_H$ and let $m_1 := reg(\mathcal{I}_H)$ Then
>
> $$reg(\mathcal{I}) \leq m_1 + h^1\mathcal{I}(m_1 - 1).$$

Again the first cohomology group causes the "problems" to connect the regularity of the curve to the regularity of its hyperplane section , as it causes problems to lift curves containing the hyperplane section of $\mathscr{C}_i$ to surfaces containing $\mathscr{C}_i$.
So, if we were able to verify that $h^1\mathcal{I}_{\mathscr{C}_i}(m_1-1)=0$, then we immediately have that the regularity of $\mathscr{C}_i$ is equal to the regularity of its generic plane section ($\mathscr{C}_i$ is assumed to be reduced, irreducible and non-degenerate). But we can not hope to be able to compute the dimension of this cohomology group for a component $\mathscr{C}_i$ if we only know the equations defining the complete intersection $\mathscr{C}$ and the points of $\mathscr{C}_i \cap H$.

Many authors quested for bounds on the regularity of an ideal $\mathfrak{a}$ using the degrees of the defining equations of the ideal: see for instance [3], [12], [13].

In particular, for our aims, the main theorem of [11] gives a linear bound in the degrees of the generators of $\mathfrak{a}$ with some hypothesis on the singularities of the primary components of $\mathfrak{a}$.

Theorem 3.3.4 ([11], Theorem 4.4)**.** *Consider $\overline{R}=\mathbb{K}[X_0,\dots,X_n]$ and $\mathfrak{a}\subseteq\overline{R}$ be a homogeneous ideal with homogeneous generators of degrees $d_1>\cdots>d_s$.*
Consider $r\leq s$ and $\mathfrak{b}\subseteq\overline{R}$, an intersection of isolated primary components of codimension r of $\mathfrak{a}$. Let S and Z be the projective schemes defined by $\mathfrak{b}$ and $\mathfrak{a}$ respectively and assume that,

1. *Z has at most isolated singularities on S,*
2. *S does not meet the other components of Z.*

Then

$$\operatorname{reg}(\mathfrak{b}) \leq (\dim_{proj}\mathfrak{b})(d_1+\cdots+d_r-r-1)+1.$$

In our setting, assume that we consider $\mathfrak{a}$ ideal of $\overline{R}$.Let $\mathfrak{q}_i$ be a primary component of $\mathfrak{a}$ of (affine) dimension 1. Then, if $\mathfrak{q}_i$ has multiplicity 1, then $\mathfrak{q}_i$ respects condition 1 of Theorem 3.3.4.

Condition 2 of Theorem 3.3.4 is never satisfied for complete intersection curves in $\mathbb{P}^3$: in fact if $\mathfrak{a}$ defines a curve in $\mathbb{P}^3$ and $\mathfrak{a}$ is not prime, then any irreducible component of the curve meets another one since the curve is connected. For a non-complete intersection ideal $\mathfrak{a}$ in $\mathbb{K}[X,Y,Z,W]$, if a primary component $\mathfrak{b}$ satisfies 1 and 2 of Theorem 3.3.4, then $\operatorname{reg}\mathfrak{b} \leq 2(d_1+d_2-2)+1 = 2d_1+2d_2-3$, where d_1 and d_2 are the highest degree of the generators of $\mathfrak{a}$.
For an ideal $\mathfrak{a}$ defining a curve in $\mathbb{P}^N$, $N \geq 4$, if a primary component $\mathfrak{b}$ satisfies 1 and 2 of Theorem 3.3.4, then we have that

$$\operatorname{reg}(\mathfrak{b}) \leq 2(\sum_{i=1}^{N-2} d_i - N - 1).$$

This bound is much better than (3.3.2) since it is linear in the degrees of the polynomials defining ideal $\mathfrak{a}$, but in practice it is not that useful, since we need to know a priori that the component $V(\mathfrak{b})$ does not intersect the other components of the curve.

Finally, for what follows, it is useful to see a bound on the regularity of a curve involving another invariant of the curve itself. We will be able to give a clear meaning to this in the next section.

Definition 3.3.5. *For any homogeneous ideal $\mathfrak{a} \subseteq \overline{R}$, we let $H_{\overline{R}/\mathfrak{a}}(t) := \dim_k \overline{R}/\mathfrak{a}_t$ be the* Hilbert function *of $\overline{R}/\mathfrak{a}$.*
For $t >> 0$, $H_{\overline{R}/\mathfrak{a}}(t) = P_{\overline{R}/\mathfrak{a}}(t)$ where $P_{\overline{R}/\mathfrak{a}}(X) \in \mathbb{K}[X]$ is the Hilbert polynomial *of $\overline{R}/\mathfrak{a}$.*
The regularity *of $H_{\overline{R}/\mathfrak{a}}$ is $\rho_{\overline{R}/\mathfrak{a}} = \min\{\bar{t} | H_{\overline{R}/\mathfrak{a}}(t) = P_{\overline{R}/\mathfrak{a}}(t) \forall t \geq \bar{t}\}$.*

If $\mathfrak{a} = I(\mathscr{C})$ is the defining ideal of a curve $\mathscr{C} \in \mathbb{P}^N$, we simply write $\rho_{\mathscr{C}}$ for $\rho_{\overline{R}/\mathfrak{a}}$.

Proposition 3.3.6 ([17], Proposition 3.4)**.** *Let $d_1 \geq \cdots \geq d_{N-1}$ be degrees for which there exists a complete intersection $Y \subseteq \mathbb{P}^N$ of type $(d_1, \ldots, d_{N-1})$ containing $\mathscr{C}$. So*

1. *$reg(I(\mathscr{C})) \leq \max\{\rho_{\mathscr{C}} + 1, \sum_{i=1}^{N-1} d_i - N + 2\}$;*
2. *if $\mathscr{C} \cap H$, with H generic plane, is not a complete intersection of type $(d_1, \ldots, d_{N-1})$ (e.g. if $\deg(\mathscr{C}) < \sum_{i=1}^{N-1} d_i$), then $reg(I(\mathscr{C})) \leq \max\{\rho_{\mathscr{C}} + 1, \sum_{i=1}^{N-1} d_i - N + 1\}$.*

We want to underline the fact that this bound holds for curves in $\mathbb{P}^N$, also for a non-equidimensional curve. We then are interested in studying methods to compute $\rho_{\mathscr{C}}$ and this is what we will see in the next section.

3.4 Generic Initial Ideal

As we have just said, it is not easy to deal with the regularity of an ideal. Anyway there is simple computational tool which allows us to compute not only the regularity but also

another interesting invariant if we look at our curves in $\mathbb{P}^N$ (instead of remaining in the affine space $\mathbb{C}^N$). We now work in the polynomial graduated ring $\overline{R} = \mathbb{C}[X_0, X_1, \ldots, X_n]$ with maximal ideal $\mathfrak{m} = (X_0, X_1, \ldots, X_n)$.

Definition 3.4.1. *A homogeneous ideal* $\mathfrak{a} \subseteq \overline{R}$ *is* saturated *if* $(\mathfrak{a} : \mathfrak{m}) = \mathfrak{a}$.

The saturation *of* $\mathfrak{a}$ *is*

$$\mathfrak{a}^{sat} = \bigcup_{k \geq 0} (\mathfrak{a} : \mathfrak{m}^k).$$

$\mathfrak{a}$ *is* m-saturated *if* $\mathfrak{a}_d = \mathfrak{a}_d^{sat}$ *for all* $d \geq m$.

The satiety *of* $\mathfrak{a}$ *is the smallest* m *for which* $\mathfrak{a}$ *is* m*-saturated.*

Proposition 3.4.2. *An ideal* $\mathfrak{a}$ *is* m*-regular if and only if* $\mathfrak{a}$ *is* m*-saturated and its sheafification* $\mathcal{I}(\mathfrak{a})$ *is* m*-regular.*

Proof. See [35], Proposition 2.6 page 139. □

From now on we will consider the polynomials in $\overline{R}$ with th *DegRevLex* term order with any order on the variables such that X_0 is the smallest one.

$$\mathbf{X^a} > \mathbf{X^b} \iff \sum a_i > \sum b_i \text{ or } a_i = b_i \text{ for } i > i_0 \text{ and } a_{i_0} < b_{i_0}.$$

Theorem 3.4.3. *[Galligo's Theorem, [35], Theorem 1.27 page 129]*

Fix any monomial order and let $\mathfrak{a}$ *be a homogeneous ideal in* $\overline{R}$*. There is a Zariski open subset* $U \subseteq GL(N+1)$ *fixed by the invertible lower triangular matrices and with non trivial intersection with the subgroup upper triangular matrices with* 1*'s on the diagonal and there is a monomial ideal* $\mathfrak{a} \subseteq R$ *, such that* $in(g(\mathfrak{a})) = \mathfrak{a}$ *for all* $g \in U$.

We will call $in(g(\mathfrak{a}))$ generic initial ideal *of* $\mathfrak{a}$*, briefly* $gin(\mathfrak{a})$.

If we make the computational effort to write down $gin(\mathfrak{a})$, then we immediately have a lot of information about the regularity and satiety of the ideal $\mathfrak{a}$.

For $\mathfrak{a}, \mathfrak{b}$ ideals, we write $\mathfrak{a}_\mathfrak{b}$ meaning the quotient $\mathfrak{a} + \mathfrak{b}/\mathfrak{b}$.

Properties 3.4.4 ([35], Theorem 2.30 page 146)**.**

1. $sat(\mathfrak{a})$ *is the degree of the highest generator of* $gin(\mathfrak{a})$ *involving* X_0*;* $reg(\mathfrak{a})$ *is the degree of the highest generator of* $gin(\mathfrak{a})$*;*

2. $\mathfrak{a}$ *is saturated if no generator of* $gin(\mathfrak{a})$ *involves* X_0*;*

3. *for a general hyperplane* H*,* $gin(\mathfrak{a}_H) = (gin(\mathfrak{a}))_{X_0}$*;*

4. *for a general hyperplane* H*,* $reg(\mathfrak{a}) = \max\{sat(\mathfrak{a}), reg(\mathfrak{a}_H)\}$.

If we consider a curve $\mathscr{C}$ in $\mathbb{C}^3$ and we consider $I(\mathscr{C}) \subseteq \mathbb{C}[X,Y,Z]$, homogenizing a set of generators with W and saturating with respect to this new variable, we obtain the homogeneous ideal $\mathfrak{a}$; we keep on writing $\mathscr{C}$ for the curve $V(\mathfrak{a}) \subseteq \mathbb{P}^3$. We can then give a representation of $gin(\mathfrak{a})$, "drawing" it in a 3-dimensional space. In fact, $\mathfrak{a}$ is saturated and so the monomial generators of its generic initial ideal does not contain the smallest variable, W (Property 3.4.4, 2.).

We now define in a proper way the concept of stair of an ideal.

Definition 3.4.5. *Let $\mathfrak{a}$ be a homogeneous ideal in $\mathbb{C}[X_0,\dots,X_n]$ and consider $gin(\mathfrak{a}) = (m_1,\dots,m_r)$. The* stair *of the ideal $\mathfrak{a}$ is the set of monomials m which are not divided by the m_i's, that is*

$$E := \{m \mid m_i \nmid m,\ i = 1,\dots,r\}.$$

There is a simple and very nice characterization for the stair of a complete intersection. In the following theorem we consider a graded ring $\overline{R}$ with n indeterminates; we use the DegRevLex term-order with an ordering on variables such that $X > Y$ are the biggest ones.

Theorem 3.4.6 ([28])**.** *If we consider a complete intersection homogeneous ideal $(F,G) \subseteq \overline{R}$ with $\deg F = d_1$ and $\deg G = d_2$, $d_1 \geq d_2$, then the generic initial ideal with respect to the DegRevLex order is*

$$gin(F,G) = (X^{d_2}, X^{d_2-1}Y^{d_1-d_2+1}, \dots, XY^{d_1+d_2-3}, Y^{d_1+d_2-1})$$

and in particular we have that $lt(g(F)) = X^{d_1-1}Y^{d_2-d_1-1}$ and $lt(g(G)) = X^{d_1}$, with g in the Zariski open subset of U of 3.4.3.

Example 3.4.7. *Considering the ideal $\mathfrak{a}$ of Example 3.1.1, $gin(\mathfrak{a}) = (X^3, X^2Y, XY^3, Y^5)$ and $gin(\mathscr{C}_1) = (X^3, X^2Y, XY^2, Y^3, X^2Z^2)$. We represent their stairs in Figure 3.1.*

The stair of an ideal $\mathfrak{a}$ is a basis for the vector space $R/g(\mathfrak{a}) = R/in(g(\mathfrak{a})) = R/gin(\mathfrak{a})$ for $g \in U \subseteq GL(N+1)$, so we can actually compute the Hilbert function of $\mathfrak{a}$ from its stair.

Furthermore, for any curve $\mathscr{C} \subseteq \mathbb{P}^3$, we have that $gin(I(\mathscr{C})_H) = gin(I(\mathscr{C}))_W$ (Property 3.4.4, 3.), but since $I(\mathscr{C})$ is saturated, $gin(I(\mathscr{C})_H) = gin(I(\mathscr{C}))$. On the other hand, if we consider the general plane H defined by $Z = 0$, we have that $I(\mathscr{C})_H$ is not saturated (as ideal in $\mathbb{C}[X,Y,W]$). Its saturation is exactly $I(\mathscr{C} \cap H)$ and then we have that $gin(I(\mathscr{C} \cap H)) \supseteq gin(I(\mathscr{C})_H)$ in $\mathbb{C}[X,Y,W]$ and so the opposite inclusion of stairs.
We finally observe that the stair of $I(\mathscr{C} \cap H)$ is exactly the one we obtain looking at the monomials in X and Y when the exponent of Z is "big enough" (looking at Figure 3.1, the dashed part obtained considering monomial with the exponent of Z bigger than 2).

If $\mathscr{C} = V(F,G) = \mathscr{C}_1 \cup \dots \cup \mathscr{C}_s$, then $E(I(\mathscr{C}_i)) \subsetneq E(I(\mathscr{C}))$. This may help us to bound the degree of a minimal generator of the ideal $I(\mathscr{C}_i)$, but it is still not sufficient.

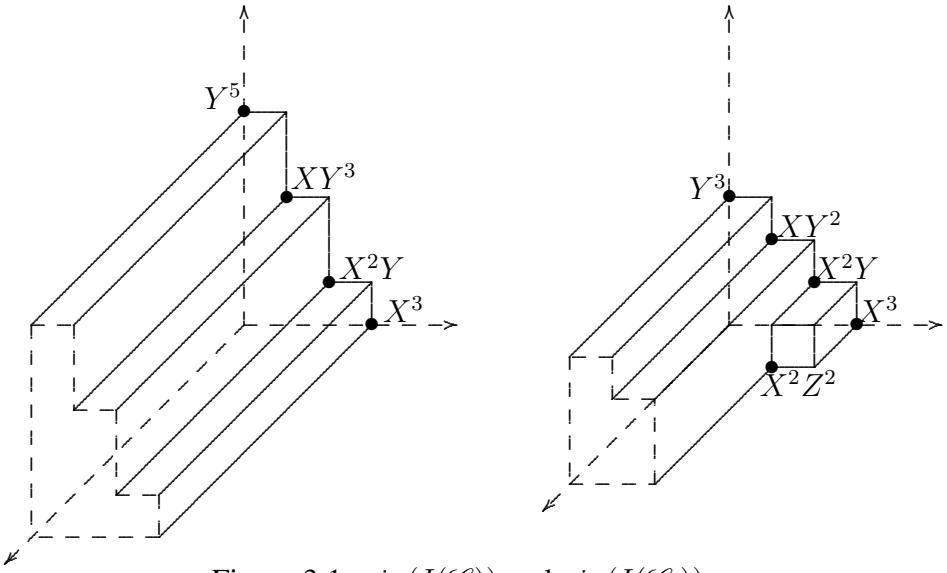

Figure 3.1: $gin(I(\mathscr{C}))$ and $gin(I(\mathscr{C}_1))$

In fact the inclusion $E(\mathscr{C}_i) \subsetneq E(\mathscr{C})$ gives us a bound about the generators of the generic initial ideal $I(\mathscr{C}_i)$ containing only X and Y, but we cannot say anything about the degree of the generators of $gin(I(\mathscr{C}_i))$ containing Z.

Finally, if $\mathfrak{a} \subseteq \mathbb{Q}[X, Y, Z]$ and we consider its homogenization in $\mathbb{C}[X, Y, Z, W]$ (keeping on using $\mathfrak{a}$ to denote it), $gin(\mathfrak{a})$ allows us not only to compute the Hilbert function, but also the Hilbert Polynomial and the regularity of the Hilbert function.

But this very "easy" way to compute the regularity of the Hilbert function of an ideal also says that in general we cannot hope to find a nice bound on the regularity of a primary component $\mathfrak{b}$ of $\mathfrak{a} = (F, G)$ if we only know $\mathfrak{a}$: in fact the bound of Proposition 3.3.6 clearly says that the regularity of the Hilbert function plays a key role in bounding the regularity of the ideal, but actually we cannot detect a priori in which cases the degrees of the generators of $\mathfrak{a}$ are sufficient to bound the regularity.

Example 3.4.8. *We again consider the complete intersection curve of Example 3.1.1, its stair and the stair of its irreducible component $\mathscr{C}_1$ (Example 3.4.7).*

Computing the Hilbert function and the Hilbert polynomial of $I(\mathscr{C}_1)$ from the generic initial ideal of $\mathscr{C}_1$, we have $\rho_{\mathscr{C}_1} = 3$. In this case the bound on regularity of Proposition 3.3.6 holds using the value $d_1 + d_2 - 1$ which actually bounds the regularity of $\mathscr{C}_1$, while $\rho_{\mathscr{C}_1}$ does not. Again, this is not the sharpest bound we hope for, since the regularity of $\mathscr{C}_1$ is 4 and the minimal degree of a generator of $I(\mathscr{C}_1)$ is 3; furthermore, there is no way to compute $\rho_{\mathscr{C}_1}$ directly from $\mathfrak{a}$, so a priori we do not know if $d_1 + d_2 - 1$ actually bounds the regularity of $I(\mathscr{C}_1)$.

3.5 Practical bounds

In the end of this chapter, we will summarize the previously discussed bounds for the degree of the minimal generator of a primary component of a complete intersection ideal in $\mathbb{Q}[X, Y, Z]$, pointing out if this bound holds for the non-complete intersection case, for curves in higher dimensional spaces and which computations are necessary (assuming, if suitable, that we performed a generic change of coordinates).

Given $\mathfrak{a} = (F, G) \subseteq \mathbb{Q}[X, Y, Z]$, we will use (as previously) the notations $d_1 = \deg F$, $d_2 = \deg G$; we will write $\mathfrak{a} \subseteq \mathbb{Q}[X, Y, Z, W]$ considering the homogenization of F and G and saturating with respect to W the ideal they generate. The degree of a separator polynomial of $\mathscr{C}_i$ is q_i.

Bounds using the Lifting Problem

We compute the set of points of $P = V(\mathfrak{a} + (h))$ where $h \in \mathbb{Q}[X, Y, Z]$ is a generic linear form defining a plane H. We compute the partition of the set P (using for instance the technique in [29]), obtaining $P_i = \{p_{ij}\}_{j=1,\ldots,\deg C_i} = \mathscr{C}_i \cap H$.

Assume that the component $\mathscr{C}_i$ is reduced and non-degenerate. Let t_i be the minimal degree of a curve of the plane H containing the set of points P_i. One of the following holds ([50], [38], [76]):

- $q_i = t_i$,
- $q_i \leq \deg \mathscr{C}_i \leq t_i^2 + 1$.

The same holds for any ideal $\mathfrak{a} \subseteq \mathbb{C}[X, Y, Z]$ with $\dim \mathfrak{a} = 1$.

The results about the Lifting problem for higher dimensional spaces do not concern the case of curves.

Bounds using regularity

For a reduced component $\mathscr{C}_i$ of $V(\mathfrak{a})$ we have ([37]):

- $q_i \leq d_1 d_2 - 1$.

The same holds for any ideal $\mathfrak{a}$, assuming that d_1 and d_2 are the highest degrees of its generators.

If we know the degree of the irreducible component $\mathscr{C}_i$, then

- $q_i \leq \deg \mathscr{C}_i - 1$.

If we know that m_1 is the regularity of the generic plane section of $\mathscr{C}_i$ and that $h^1\mathcal{I}_{\mathscr{C}_i}(m_1 - 1) = 0$, then ([58])

- $q_i \leq m_1$.

If $\mathscr{C}_i$ is reduced and we are able to compute $\rho_{\mathscr{C}_i}$, regularity of the Hilbert function of a component $\mathscr{C}_i$ of $\mathscr{C}$, then ([17])

- $q_i \leq \max\{\rho_{\mathscr{C}_i}, d_1 + d_2 - 1\}$

This is true also for a reduced component $\mathscr{C}_i$ of the complete intersection curve $\mathscr{C} \subseteq \mathbb{P}^N$: $q_i \leq \max\{\rho_{\mathscr{C}} + 1, \sum_{i=1}^{N-1} d_i - N + 2\}$

If we consider $\mathfrak{a} \subseteq \mathbb{C}[X_1, \ldots, X_N]$, with $N \geq 3$ and $\mathfrak{a}$ non-complete intersection or $N \geq 4$, if we are able to verify that the primary component $\mathfrak{q}_i$ has multiplicity one and $V(\mathfrak{q}_i)$ does not meet the other components of the curve $V(\mathfrak{a})$, then we have ([11])

- $q_i \leq 2(\sum_{i=1}^{N-2} d_i - N - 1)$

with d_i's degrees of the generators of $\mathfrak{a}$, $d_1 \geq \cdots \geq d_r$.

Bounds using the Generic Initial Ideal

If $\mathscr{C}_i$ is a reduced component of $\mathscr{C}$ and we are able to compute $gin(I(\mathscr{C}_i)_H)$, with H general hyperplane in $\mathbb{P}^3$, then ([35])

- $q_i \leq \max\{\deg(m_{ij})\}$,

where $(m_{i1}, \ldots, m_{ik_i})$ is the monomial basis of $gin(I(\mathscr{C}_i)_H)$. The same bound holds for the reduced component of any curve in $\mathbb{P}^N$.

In particular, for a complete intersection curve in $\mathbb{P}^3$, we find the same bound of [17].

Chapter 4

Decomposition of a complete intersection in $\mathbb{C}^3$

In the first part of this chapter, we will present an exact technique combining generic projection and absolute factorization. This technique is simple and immediate from the geometric point of view, it was first showed on the beginning of the XX-th century (see [41]). For lack of a complete and accessible reference, we will present in an exhaustive way this strategy and then modify it using modular techniques.

4.1 An exact strategy: Projection and Colon Ideals

Given an ideal $\mathfrak{a} = (F, G) \subseteq \mathbb{Q}[X, Y, Z]$ defining a curve in $\mathbb{C}^3$, we will now show an "exact" strategy to obtain the ideals defining the components, in particular for the ones of multiplicity 1. This strategy is "exact" in the sense that it uses symbolic computations and not numerical floating-points approximations, and it is quite intuitive. Actually this strategy is exact but not useful in practice: the computations needed are quite long and hard to perform. Anyway, we will investigate this method in details since later (Section 4.2) we will adapt this strategy giving up the exact computations to gain fastness, but preserving some information about the irreducible and reduced components, namely their Hilbert Function.

Part of the following lemmas and proposition can be found in [73], but here we detail the proofs for the case $n = 3$.

Definition 4.1.1. *A* linear projection *is a surjective affine map:*

$$\begin{aligned} \pi : \mathbb{C}^3 &\to \mathbb{C}^2 \\ P = (x, y, z) &\mapsto (L_1(P), L_2(P)) \quad \textit{with } L_i(X, Y, Z) = a_{i_0} + a_{i_1}X + a_{i_2}Y + a_{i_3}Z. \end{aligned} \tag{4.1.1}$$

In a similar way, we can define a projection for the projective space, considering

$$\begin{aligned} \pi_L : \mathbb{P}^3 \setminus L &\to \mathbb{P}^2 \\ P = [W : X : Y : Z] &\mapsto (L_0(P), L_1(P), L_2(P)) \end{aligned} \tag{4.1.2}$$

with $L_i(W, X, Y, Z) = a_{i_0}W + a_{i_1}X + a_{i_2}Y + a_{i_3}Z$. *$L$ is the point of intersection of the linear equations L_i and it is the* center *of the projection.*
Two projections π_1 and π_2 from $\mathbb{P}^3$ to $\mathbb{P}^2$ are equivalent *if they have the same center L.*

The geometric meaning of the projection is the following one:
once chosen the center L and a $\mathbb{P}^2 \subset \mathbb{P}^3$ such that $L \cap \mathbb{P}^2 = \emptyset$, then for any $P \in \mathbb{P}^3 \setminus L$, we consider the linear space generated by P and L, that we denote with $\langle P, L \rangle$. We then consider $\mathbb{P}^2 \cap \langle P, L \rangle$ that is a point P' on $\mathbb{P}^2$ and we define in this way $\pi_L(P) = P'$.
In general, we can consider $\mathbb{C}^N \subset \mathbb{P}^N$ thinking of $\mathbb{C}^N$ as $\mathbb{P}^N \setminus H$, where H is the hyperplane at infinity. The projections $\pi_L : \mathbb{P}^3 \setminus L \to \mathbb{P}^2$ which are extensions of projections $\pi : \mathbb{C}^3 \to \mathbb{C}^2$ are exactly the ones whose center is on the hyperplane H.

We now consider a projection $\pi : \mathbb{C}^3 \to \mathbb{C}^2$ and we restrict it to a curve $\mathscr{C}$ of $\mathbb{C}^3$. It is not always true that $\pi_{\mathscr{C}}$ is proper (the preimage of a compact subset is a compact): for instance, the projection of the hyperbola defined by the ideal $(XY - 1, Z = 0)$ on the the plane $\{X = 0\}$ is the Y-axis without the origin, so the restriction of π to the hyperbola is not proper.

Proposition 4.1.2 ([73], Lemma 5.1)**.** *Let $\mathscr{C}$ be a curve in $\mathbb{C}^3$ all of whose irreducible components are of dimension 1. For a general linear projection $\pi : \mathbb{C}^3 \to \mathbb{C}^2$, the map $\pi_{\mathscr{C}}$ is proper and generically one-to-one.*
In particular $\pi(\mathscr{C})$ is a closed subvariety of $\mathbb{C}^2$ of degree equal to the degree of $\mathscr{C}$.

Proof. Without loss of generality, we can assume that $\mathscr{C}$ is irreducible.

The properness of $\pi_{\mathscr{C}}$ follows from Noether Normalization Theorem (see [25], Theorem 13.3).

Let $\overline{\mathscr{C}}$ be the closure in $\mathbb{P}^3$ of $\mathscr{C}$ in the complex topology. $\overline{\mathscr{C}}$ is a 1-dimensional subvariety of $\mathbb{P}^3$ and $\mathscr{C}$ is a Zariski open subset of $\overline{\mathscr{C}}$.
As pointed out above, a linear projection $\pi : \mathbb{C}^3 \to \mathbb{C}^2$ is the restriction of a projection $\pi_P : \mathbb{P}^3 \to \mathbb{P}^2$ whose center P lies on the hyperplane at infinity H, $H := \mathbb{P}^3 \setminus \mathbb{C}^3$.
Let Δ be the diagonal of $\mathscr{C} \times \mathscr{C}$. We can define an algebraic map $\phi : \mathscr{C} \times \mathscr{C} \setminus \Delta \to H$: (P_1, P_2) is sent to the intersection of H with the projective line passing through P_1 and P_2.

Suppose now that all of the projections π_P with $P \in H \setminus \overline{\mathscr{C}}$ are not generically one to one, then we can conclude that the fiber of ϕ over each point of $H \setminus (\overline{\mathscr{C}} \setminus \mathscr{C})$ is at least 1-dimensional.

Then we have

$$2{\cdot}1 = \dim(\mathscr{C}\times\mathscr{C}) = \dim(\mathscr{C}\times\mathscr{C}\setminus\Delta) \geq 1{+}\dim\phi(\mathscr{C}\times\mathscr{C}\setminus\Delta) \geq 1{+}\dim(H\setminus(\overline{\mathscr{C}}\setminus\mathscr{C})) = 1{+}2$$

But this is contradictory, so the dimension of the generic fiber of ϕ is less than 1, and so there is a Zariski open set of $H \setminus (\overline{\mathscr{C}} \setminus \mathscr{C})$ such that the associated projections are generically one-to-one.

For what concerns the degree, it is sufficient to prove for a generic linear projection in projective space. Indeed, $\deg\mathscr{C} = \deg\overline{\mathscr{C}}$, $\deg\pi(\overline{\mathscr{C}}) = \deg\overline{\pi(\mathscr{C})}$ and $\pi(\overline{\mathscr{C}}) = \overline{\pi(\mathscr{C})}$.

Let V be the subvariety of $\pi(\mathscr{C})$ obtained as the union of the singular points of $\pi(\mathscr{C})$ and the image under π of the ramification locus of π. If we consider a general line L, L meets $\overline{\pi(\mathscr{C})}$ transversely in $\deg(\overline{\pi(\mathscr{C})})$ points contained in $\pi(\overline{\mathscr{C}})\setminus V$. Then the 2-dimensional linear space $\pi^{-1}(L)$ meets $\overline{\mathscr{C}}$ transversely in $\deg\overline{\mathscr{C}}$ points contained in the regular points of $\overline{\mathscr{C}}$. □

Corollary 4.1.3. *Let $\pi : \mathbb{C}^3 \to H$ be a projection, with H plane in $\mathbb{C}^3$.*

1. *If $\mathscr{C}_i$ and $\mathscr{C}_j$ are two distinct irreducible components of $\mathscr{C}$, then $\pi(\mathscr{C}_i) \neq \pi(\mathscr{C}_j)$;*
2. *If we consider a generic linear projection, $\mathscr{C}$ is irreducible if and only if the polynomial defining $\pi(\mathscr{C})$ is absolutely irreducible;*
3. *If $D(T_1, T_2)$ is the polynomial defining the projection $\mathscr{D} := \pi(\mathscr{C})$ and we consider ts absolute factorization $D = D_1^{m_1}\cdots D_c^{m_c}$, then c is exactly the number of distinct irreducible components of $\mathscr{C}$, m_i is the multiplicity of the component $\mathscr{C}_i$ and $\deg D_i$ its degree.*

We now assume that we performed a generic linear change of coordinates in the sense that we homogenize F and G with respect to a new variable W, we make a generic linear change of coordinates and then we go back to the affine space, putting $W = 1$; in this way we can consider the projections on the coordinates planes to be generic and avoid problems with components at infinity.

We consider the projection $\pi_1 : \mathbb{C}^3 \to H_1$, with H_1 the plane defined by the equation $Y = 0$. We call $\mathscr{D}_1$ the projection of the curve $\mathscr{C}$ on H_1. This is a curve in the plane and its decomposition is equivalent to the absolute factorization of the bivariate polynomial $D_1(X, Z)$ defining $\mathscr{D}_1$ in the plane H_1. Furthermore, the components of $\mathscr{D}_1$ are in one-to-one correspondence with the irreducible components of $\mathscr{C}$.

If $D_1 = D_{11}^{m_1}\cdots D_{1c}^{m_c}$, each factor D_{1j} defines in $\mathbb{C}^3$ a ruled surface, a cylinder, containing the component $\mathscr{C}_j$. We can then start considering the ideal $(F, G, D_{1j}^{m_j})$. But $V(F, G, D_{1j}^{m_j})$ contains not only the component $\mathscr{C}_j$, but also the points of the sets $V(D_{1j}^{m_j}) \cap \mathscr{C}_k$ for $k \neq j$.

We pass again to consider the problem from the algebraic point of view, using the primary decomposition of an ideal, whose main definitions and properties were already recalled in Section 2.1.

Consider the ideal $\mathfrak{a} = (F, G) \subseteq \mathbb{Q}[X, Y, Z]$, assume that we performed a generic change of coordinates with integer coefficients and consider its primary decomposition

$$\mathfrak{a} = \bigcap_{i=1}^{c} \mathfrak{q}_i,$$

where each primary ideal $\mathfrak{q}_i \in \mathbb{C}[X, Y, Z]$ is an algebraic component of $\mathfrak{a}$.

Thanks to the generic change of coordinates, we can consider the projection on the coordinate plane H_1 (of equation $Y = 0$) as a generic one and compute the polynomial D_1 representing the projection of $\mathscr{C}$ on H_1 through a resultant: $D_1 = Res_Y(F, G)$. We compute the absolute factorization of D_1, so that each absolute factor $D_{1j}^{m_j}$ is the equation of a cylinder containing an irreducible component of $V(\mathfrak{a})$

If we consider the ideal $\mathfrak{a}+(D_{1j}^{m_j}) = (F, G, D_{1j}^{m_j})$, we have that its primary decomposition is

$$\mathfrak{a} + (D_{1j}^{m_i}) = \bigcap_{i=1}^{s} \left(\mathfrak{q}_i + (D_{1j}^{m_j})\right)$$

where, by construction, D_{1j} is absolutely irreducible, so the ideal $\mathfrak{q}_i+(D_{1j}^{m_j})$ is $(\mathfrak{p}_i + (D_{1j}))$-primary.

Thinking of the corresponding varieties $V(\mathfrak{q}_i)$ and $V(D_{1j}^{m_j})$, the ideal $\mathfrak{q}_i + (D_{1j}^{m_j})$ is:

- (1) when $V(\mathfrak{q}_i) \cap V(D_{1j}^{m_j}) = \emptyset$;
- an ideal of dimension 0 when $V(\mathfrak{q}_i) \cap V(D_{1j}^{m_j})$ is a finite set of points;
- an ideal of dimension 1 if $V(\mathfrak{q}_i) \cap V(D_{1j}^{m_j})$ contains the irreducible component $\mathscr{C}_j$ (and in this case we write $i = j$). Obviously in this case $\mathfrak{q}_j + (D_{1j}^{m_j}) = \mathfrak{q}_j$ and $\mathfrak{p}_j + (D_{1j}^{m_j}) = \mathfrak{p}_j$

Finally, the ideal $\mathfrak{a} + (D_{1j}^{m_j})$ "describes" the component $\mathscr{C}_j$ with some extra points. In order to avoid these extra points, we can repeat the same procedure with another generic projection π_2 from $\mathbb{C}^3$ onto the plane H_2. Thanks to the generic coordinates chosen, we can use again a coordinate plane and a resultant, choosing H_2 defined by the equation $Z = 0$. If we consider $\pi_2(\mathscr{C}) = \mathscr{D}_2$, the polynomial defining $\mathscr{D}_2$ on H_2 is again a bivariate polynomial $D_2 = Res_Z(F, G)$. We compute its absolute factorization and we obtain another cylinder containing $\mathscr{C}_j$, defined by the factor D_{2j}.

Remark 4.1.4. *Actually, in the absolute factorizations of D_1 and D_2 there may be several factors with the same degrees and multiplicity. For instance, this happens when one of the components $\mathscr{C}_j$ is a non-purely rational component (see Definition 2.2.2).*

In order to match the factors defining the cylinders containing the same component, we can look at the Hilbert dimension of the ideal $(F, G, D_{1j}^{m_j}, D_{2i}^{m_i})$. This dimension is 1 if

and only if $D_{1j}^{m_j}$ and $D_{2i}^{m_i}$ contain the same irreducible component of $\mathscr{C}$; this follows from Corollary 4.1.3, 1.

In order to find the correct couples $(D_{1j}^{m_j}, D_{2j}^{m_j})$, we will not compute all of the Hilbert dimensions of the ideals $\mathfrak{a} + (D_{1j}^{m_j}) + (D_{2i}^{m_i})$. We will compute the Hilbert dimension only for the couples such that $\deg D_{1j} = \deg D_{2i}$ and $m_j = m_i$. Furthermore, we get an almost certain probabilistic check by considering a generic plane section: that is, we can look for the couples $D_{1j}^{m_j}, D_{2i}^{m_i}$ such that the ideal $(F, G, D_{1j}^{m_j}, D_{2i}^{m_i})$ with one variable specialized (e.g. $X = x_0 \in \mathbb{Z}$) is zero-dimensional and nonempty (see Algorithm 7).

Once that we matched $D_{1j}^{m_j}$ and $D_{2j}^{m_j}$ (after re-indexing of the factors), the variety defined by $\mathfrak{a}_j = \mathfrak{a} + (D_{1j}^{m_j}) + (D_{2j}^{m_j})$ is "almost" $\mathscr{C}_j$: we will still have some extra points, "embedded points", which are in $V(D_{1j}) \cap V(D_{2j}) \cap \mathscr{C}_k$ for $k \neq j$. Actually these points are in $\mathscr{C}_j \cap \mathscr{C}_k$, for $k \neq j$.

Lemma 4.1.5. *Consider two general projections π_1 and π_2 from $\mathbb{C}^3$ to the planes H_1 and H_2, H_1, H_2 non-parallel. Consider two distinct curves $\mathscr{C}_1$ and $\mathscr{C}_2$. If there are points $P_1 \in \mathscr{C}_1$ and $P_2 \in \mathscr{C}_2$ such that we have*

$$\pi_1(P_1) = \pi_1(P_2) \qquad \pi_2(P_1) = \pi_2(P_2).$$

Then $P_1 = P_2$ is a point in $\mathscr{C}_1 \cap \mathscr{C}_2$.

Proof. We can write $\pi_1(P) = (L_1^{(1)}(P), L_2^{(1)}(P))$ and $\pi_2(P) = (L_1^{(2)}(P), L_2^{(2)}(P))$ with $L_i^{(j)} = a_{i0}^{(j)} + a_{i1}^{(j)}X + a_{i2}^{(j)}Y + a_{i3}^{(j)}Z$. Remark that since a projection is a surjective map, $L_1^{(j)} \neq L_2^{(j)}$, $j = 1, 2$, and since the planes are not parallel the matrix whose rows are the four vectors $(a_{i1}^{(j)}, a_{i2}^{(j)}, a_{i3}^{(j)})$ has rank 3.

P_1 and P_2 have the same image under π_1 and π_2 if and only if $L_i^{(j)}(P_1) = L_i^{(j)}(P_2)$, $i, j \in \{1, 2\}$. We obtain 4 equations of kind

$$a_{i1}^{(j)}(x_1 - x_2) + a_{i2}^{(j)}(y_1 - y_2) + a_{i3}^{(j)}(z_1 - z_2) = 0, \quad P_l = (x_l, y_l, z_l), l = 1, 2.$$

The unique solution to this system of equations (since we assumed that H_1 and H_2 are not parallel) is the trivial one, and so we have that $P_1 = P_2$ is a point of $\mathscr{C}_1 \cap \mathscr{C}_2$. □

So, for the moment, we have an ideal such that its set of zeros contains the variety $\mathscr{C}_j$ but has some embedded points, the set $\mathcal{P}$; we now show that this finite set of points is also contained in the zeros of the singular locus of $\mathfrak{a}_j$ (Definition 4.1.6).
Considering again primary decompositions, for what concerns $\mathfrak{a}_j$ we have that:

$$\mathfrak{a}_j = \mathfrak{a} + (D_{1j}^{m_j}) + (D_{2j}^{m_j}) = \bigcap_{i=1}^{l} (\mathfrak{q}_i + (D_{1j}^{m_j}) + (D_{2j}^{m_j})) \tag{4.1.3}$$

where $\mathfrak{q}_i + (D_{1j}^{m_j}) + (D_{2j}^{m_j})$ is a $(\mathfrak{p}_i + (D_{1j}) + (D_{2j}))$-primary ideal.
For $i = j$, $\mathfrak{p}_j + (D_{1j}) + (D_{2j}) = \mathfrak{p}_j$ has dimension 1 and its set of zeros is the component $\mathscr{C}_j$. For $i \neq j$, $\mathfrak{q}_i + (D_{1j}) + (D_{2j})$ has dimension 0 (or -1, if the associated set of zeros is empty).

In particular, the points of $\mathscr{C}_j \cap \mathscr{C}_k$, with $j \neq k$ correspond to the primary components of $\mathfrak{a}_j$ of dimension 0. This components are in the *singular locus* of $\mathbb{C}[X, Y, Z]/\mathfrak{a}$.

Here we just recall the algebraic definition of singular locus and the useful Jacobian criterion.

Definition 4.1.6. *Let $\mathfrak{a}$ be an ideal of $\mathbb{K}[X_1, \ldots, X_n]$, $\mathbb{K}$ perfect field, $\mathfrak{a} = (f_1, \ldots, f_s)$. A prime ideal $\mathfrak{p}$ containing $\mathfrak{a}$ is in the* singular locus *of $\mathbb{K}[X_1, \ldots, X_n]/\mathfrak{a}$ if the localization of $\mathbb{K}[X_1, \ldots, X_n]/\mathfrak{a}$ at $\mathfrak{p}$ is not a regular local ring.*

With an abuse of notation, we will say "singular locus of $\mathfrak{a}$" for the singular locus of $\mathbb{K}[X, Y, Z]/\mathfrak{a}$.

Proposition 4.1.7 ([25], Corollary 16.20)**.** *Let $\mathfrak{a}$ be an ideal of $\mathbb{K}[X_1, \ldots, X_n]$, $\mathbb{K}$ perfect field, $\mathfrak{a}$ of pure codimension c, $\mathfrak{a} = (f_1, \ldots, f_s)$. Let J be the ideal generated by the $c \times c$-minors of the Jacobian Matrix $(\partial f_i/\partial X_j)$. Then J defines the singular locus of $\mathfrak{a}$: a prime $\mathfrak{p}$ contains J if and only if $\mathfrak{p}$ is in the singular locus of $\mathfrak{a}$.*

We can then compute easily the equations defining the singular locus of $\mathfrak{a}$:

- Compute the jacobian matrix of the ideal (F, G);
- Compute M_1, M_2, M_3, the 2×2 minors of the jacobian matrix;
- The singular locus of the curve is defined by $V(M_1, M_2, M_3)$.

We are then interested in considering $\mathfrak{a}_j$ and removing the "embedded" primary components corresponding to $\mathcal{P} \subseteq V(M_1, M_2, M_3)$.

We can do this for the irreducible components obtained from irreducible factors of multiplicity 1 through the computation of a colon ideal.

In general, for $\mathfrak{a}_1, \mathfrak{a}_2$ ideals in a ring R:

$$(\mathfrak{a}_1 : \mathfrak{a}_2) = \{f \in R | f \cdot \mathfrak{a}_2 \subseteq \mathfrak{a}_1\}$$

If we consider an ideal generated by an element of R, we will simply write $(\mathfrak{a} : f)$ instead of $(\mathfrak{a} : (f))$.

Lemma 4.1.8 ([2], Lemma 4.4.)**.** *Let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal, f an element of R. Then*

1. *if $f \in \mathfrak{q}$ then $(\mathfrak{q} : f) = (1)$;*

2. *if* $f \notin \mathfrak{q}$ *then* $(\mathfrak{q} : f)$ *is* $\mathfrak{p}$*-primary, and therefore* $\sqrt{(\mathfrak{q} : f)} = \mathfrak{p}$*;*

3. *if* $f \notin \mathfrak{p}$ *then* $(\mathfrak{q} : f) = \mathfrak{q}$.

Proposition 4.1.9. *In the previous setting, if* D_{1j}, D_{2j} *are factors of multiplicity one of* D_1 *and* D_2 *resp., such that the set of zeros of* $\mathfrak{a}_j := \mathfrak{a} + (D_{1j}) + (D_{2j})$ *contains* $\mathscr{C}_j$*, then* $(\mathfrak{a}_j : M_1)$ *is exactly* $\mathfrak{p}_j$*, the prime ideal defining the irreducible component* $\mathscr{C}_j$ *of* $\mathscr{C} = V(F, G)$.

Proof. Consider the primary decomposition of $\mathfrak{a}_j$ obtained by the primary decomposition of (F, G):

$$\mathfrak{a}_j = \mathfrak{a} + (D_{1j}) + (D_{2j}) = \bigcap (\mathfrak{q}_i + (D_{1j}) + (D_{2j})) .$$

Consider $\sqrt{\mathfrak{q}_i} = \mathfrak{p}_i$. For $i \neq j$, if $V(\mathfrak{q}_i + (D_{1j}) + (D_{2j}))$ is not empty, then $\mathfrak{q}_i + (D_{1j}) + (D_{2j})$ is in the singular locus of $\mathfrak{a}$; then $M_1 \in \mathfrak{p}_i + (D_{1j}) + (D_{2j})$.
For $i = j$, $M_1 \notin \mathfrak{p}_j + (D_{1j}) + (D_{2j}) = \mathfrak{p}_j$ since we assumed that the multiplicity of $\mathscr{C}_j$ is 1.

So, using Lemma 4.1.8, we have immediately that $((\mathfrak{q}_i + (D_{1j}) + (D_{2j})) : M_1)$ is the ideal (1) for all $i \neq j$, while for j, $((\mathfrak{q}_j + (D_{1j}) + (D_{2j})) : M_1) = (\mathfrak{q}_j : M_1) = \mathfrak{p}_j$. □

Remark 4.1.10. *Proposition 4.1.9 applies only for components of multiplicity 1 (that is, for factors in the absolute factorization of multiplicity 1).*
In fact, if we consider an ideal $\mathfrak{a}_j = \mathfrak{a} + (D_{1j}^{m_j}) + (D_{2j}^{m_j}), m_j \geq 2$*, we have that this ideal contains the singular locus of* (F, G)*, so* $M_1 \in \mathfrak{a}_j$ *and (using Lemma 4.1.8),* $(\mathfrak{a}_j : M_1) = (1)$.

For components of multiplicity greater than 1*, we may "clean" at least a part of the embedded points which are zeroes of the ideal* $\mathfrak{a}_j$ *in the following way:*

- *First, we use the described strategy for the components of multiplicity one, obtaining the set of prime ideals* $\{\mathfrak{p}_{i_1}, \ldots, \mathfrak{p}_{i_v}\}$ *which are the ideals for the irreducible and reduced components* $\{\mathscr{C}_{i_1}, \ldots, \mathscr{C}_{i_v}\}$

- *since we can not use the colon ideal with respect to a generator of the singular locus, we then compute*

$$\mathfrak{b} := (\cdots((\mathfrak{a}_j : f_{i_1}) : f_{i_2}) \cdots : f_{i_v}),$$

for $f_{i_j} \in \mathfrak{p}_{i_j}$.

In this way, we can already "clean" some of the embedded points. For the other points, for any component of multiplicity ≥ 2 *we should consider the corresponding* D_{1j} *and compute again some "nested" colon ideals, starting from* $\mathfrak{b}$*, with respect to the* D_{1i}*,* $i \neq j$.

4.1.1 Algorithm and discussion

In this section we will summarize the strategy of projection and quotient, writing down the main algorithm (Algorithm 6) and an auxiliary one to match the couples $D_{1j}^{m_j}, D_{2i}^{m_i}$ (Algorithm 7).

In Algorithm 7 if $V(F, G, D_{1i}^{m_j}, D_{2i}^{m_i})$ is a finite set of points, then a general plane section is empty, so the Hilbert Dimension of $(F(x_0, Y, Z), G(x_0, Y, Z), D_{1i}^{m_j}(x_0, Z), D_{2i}^{m_i}(x_0, Y))$ is generically -1.

In Algorithm 6, the Preprocessing Step allows us to consider the projections on the coordinate planes $Z = 0$ and $Y = 0$ as generic projections. We can apply the strategy presented in Section 4.1 using these projections which are easily computed through the resultant.

Algorithm 6 is exact, but in practice the computations are too hard: we did not manage to perform Algorithm 6 at Steps 2 (because of the computation and factorization of the resultant) and 6 (because of the saturation) with a standard workstation.

In the following section we will show that we can perform all these computations modulo a well-chosen prime integer p. The ouputs of the adapted versions of Algorithms 6 and 7 will be no more exact, but they will have some useful information about the ideals of the irreducible and reduced components, in particular their Hilbert functions.

This will be possible observing that the practical computations of the problematic steps of Algorithm 6 are actually obtained through Groebner Basis. We will show that a good choice of p will preserve the Groebner Basis and so the Hilbert functions of the ideals computed.

Algorithm 6 Exact Decomposition of a complete intersection

Input: $\mathfrak{a} = (F, G) \in \mathbb{Q}[X, Y, Z]$.

Output: The number of irreducible components of dimension 1, their degrees and multiplicities.

If the multiplicity of the component is 1, a system of generators of the ideal; if the multiplicity of the component is ≥ 2, two surfaces "isolating" the component from the other ones.

1: **Preprocessing:** Perform a generic integer change of coordinates on F and G.

2: Perform the absolute factorization of $D_1 := Res_Y(F, G)$ and $D_2 := Res_Z(F, G)$:

$$D_1 = D_{11}^{m_1} \cdots D_{1s}^{m_s}, \quad D_2 = D_{21}^{m_1} \cdots D_{2s}^{m_s}.$$

3: Match the D_{1j}'s and D_{2i}'s through Algorithm 7 in such a way that (after re-numbering of the factors) $\mathfrak{a}_j = (F, G, D_{1j}^{m_j}, D_{2j}^{m_j})$ contains a component.

4: **if** m_i is 1 **then**

5: Compute the Jacobian matrix of (F, G) and a minor of size 2×2, S.

6: Compute $\mathfrak{a}_j^{(S)}$ the quotient of $\mathfrak{a}_j$ with S.

7: **end if**

8: **return** for every j: $\deg D_{1j}, m_j, \mathfrak{a}_j$ (if $m_j \geq 2$) or $\deg D_{1j}$,m_j, $\mathfrak{a}_{ij}^{(S)} = I(\mathscr{C}_j)$ (if $m_j = 1$).

Algorithm 7 Matching of factors through Hilbert Dimension

Input: F, G and the absolute factors $\{D_{1j}^{m_j}(X,Z)\}_{j=1,\ldots,c}, \{D_{2j}^{m_j}(X,Y)\}_{j=1,\ldots,c}$ of $D_1(X,Z)$ and $D_2(X,Y)$ respectively.

Output: $L := [(D_{1j}^{m_j}, D_{2j}^{m_j})]_{j=1,\ldots,c}$ with $D_{1j}^{m_j}$ and $D_{2j}^{m_j}$ containing the same component $\mathscr{C}_j$ of $\mathscr{C}$.

$L :=$ empty list, $x_0 \in \mathbb{Z}$ randomly chosen integer
for i from 1 to c **do**
  $j := 1$
  while $j \leq c$ **do**
    if $\deg D_{1i} = \deg D_{2j}$ **and** $m_i = m_j$. **then**
      Compute the Hilbert Dimension h of the ideal

$$(F(x_0, Y, Z), G(x_0, Y, Z), D_{1i}^{m_i}(x_0, Z), D_{2j}^{m_j}(x_0, Y))$$

      if h=0 **then**
        add the couple $(D_{1i}^{m_i}, D_{2j}^{m_j})$ to the list L, $j := c + 1$
      else
        j:=j+1
      end if
    end if
  end while
end for
Re-number the factors of D_2 in such a way that the couples in L are of the form $(D_{1i}^{m_i}, D_{2i}^{m_i})$
return L

4.2 Good reductions

We are interested in preserving some properties of an ideal $\mathfrak{a}$ in $R = \mathbb{L}[X_1, \ldots, X_n]$ ($\mathbb{L}$ is a simple algebraic extension of $\mathbb{Q}$) "modulo" a well-chosen p. In particular, we would like the reduction modulo p to give us a bound on the degrees of the minimal generators of $\mathfrak{a}$.

We use the definitions about the affine Hilbert function at the end of Section 2.1 and we now complete them.

For a polynomial ring $\mathbb{K}[X_1, \ldots, X_n]$, we will denote with $\mathbb{T}^n$ the monoid of monomials in $\mathbb{K}[X_1, \ldots, X_n]$ and with $\mathbf{X}^I = x_1^{i_1} \cdots, x_n^{i_n}, i_j \in \mathbb{N}$ a monomial. A term ordering σ on $\mathbb{T}^n$ is *degree compatible* if for any couple of monomials $\mathbf{X}^I, \mathbf{X}^J$, $\mathbf{X}^I \geq_\sigma \mathbf{X}^J$ implies $\deg \mathbf{X}^I \geq \deg \mathbf{X}^J$.

Once fixed a term order σ on $\mathbb{T}^n$, for a polynomial $g \in \mathbb{K}[X_1, \ldots, X_n]$, we denote with $LM_\sigma(g)$ (or simply $LM(g)$ if there is no ambiguity) the maximal monomial with respect to σ appearing in g with non-zero coefficient.

Proposition 4.2.1. *Let σ be a degree compatible term ordering on $\mathbb{T}^n$.*

1. *For every $i \in \mathbb{Z}$, we have $HF^a_{R/\mathfrak{a}}(i) = \sum_{j=0}^{i} HF_{R/LM_\sigma(\mathfrak{a})}(j)$. In particular, we have $HF^a_{R/\mathfrak{a}}(i) = HF^a_{R/LM_\sigma(\mathfrak{a})}(i)$ for all $i \in \mathbb{Z}$.*

2. *Let W be a homogenizing indeterminate, and let $\overline{R} = \mathbb{K}[X_1, \ldots, X_n, W]$ be standard graded. Then we have $HF^a_{R/\mathfrak{a}}(i) = HF_{\overline{R}/\mathfrak{a}^{hom}}(i)$ for all $i \in \mathbb{Z}$.*

Proof. See [49], Proposition 5.6.3. □

Proposition 4.2.1 gives us the practical way to compute the affine Hilbert function of $\mathfrak{a}$: chosen a degree compatible term ordering σ we can compute the initial ideal of $\mathfrak{a}$, homogenize it and then compute the Hilbert function of $\overline{R}/LM(\mathfrak{a})^{hom}$.

Then we can bring back our problem about the choice of a good p with respect to the affine Hilbert function to the choice of a good p with respect to $LM_\sigma(\mathfrak{a})$, through the following well known property of Groebner Basis.

Theorem 4.2.2 (Macaulay's Basis Theorem)**.** *Let $\mathbb{K}$ be a field, let $R = \mathbb{K}[X_1, \ldots, X_n]$ be a polynomial ring over $\mathbb{K}$, let $M \subseteq R^s$ be a R-submodule, and let σ be a module term ordering on $\mathbb{T}^n\langle e_1, \ldots, e_s\rangle$. We denote the set of all terms in $\mathbb{T}^n\langle e_1, \ldots, e_s\rangle / LM_\sigma(M)$ by B.*
Then the residue classes of the elements of B form a basis of the $\mathbb{K}$-vector space R^s/M.

Let $\mathfrak{a} = (f_1, \ldots, f_s) \subseteq \mathbb{L}[X_1, \ldots, X_n]$ be an ideal. $\mathbb{L}$ is a normal algebraic extension of $\mathbb{Q}$ of degree s: $\mathbb{L} \simeq \mathbb{Q}(\alpha)$, where α is an algebraic number such that its minimal polynomial is $q(T) \in \mathbb{Q}[T]$, $\deg q(T) = s$ and $q(T) = \sum_{i=1}^{s}(T - \sigma_i(\alpha))$ where σ_i are the automorphism of $\mathbb{L}$ fixing $\mathbb{Q}$, $\sigma_i(\alpha) = \alpha_i$ are the conjugates of α over $\mathbb{Q}$.

We can write $q(T)$ as a polynomial with integer coefficients and primitive.
Consider a prime integer p such that $q(T)$ splits in $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ in the following way: $q(T) = (T - \beta_p) \cdot S(T)$ where $\deg S(T) = s - 1$, $0 \leq \beta_p \leq p - 1$ and $\gcd((T - \beta_p), S(T)) = 1$.

We then define the following map, from the extension ring $\mathbb{Z}[\alpha]$ of $\mathbb{Z}$ to the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$:

$$\begin{aligned} \psi_p : \mathbb{Z}[\alpha] &\to \mathbb{F}_p \\ \alpha &\mapsto \beta_p \\ a \in \mathbb{Z} &\mapsto a \mod p. \end{aligned} \tag{4.2.1}$$

This definition on the generators obviously extend to a homomorphism of rings, well-defined because of the choice of p and consequently of β_p.

We can then extend this homomorphism to the polynomials:

$$\psi_p : \mathbb{Z}[\alpha][X_1, \ldots, X_n] \to R_p = \mathbb{F}_p[X_1, \ldots, X_n]$$
$$f = \sum_{d=0}^{m} \sum_{i+j+k=d} a_{ijk} X^i Y^j Z^k \mapsto \tilde{f} = \sum_{d=0}^{m} \sum_{i+j+k=d} \psi_p(a_{ijk}) X^i Y^j Z^k.$$

If we consider $\mathfrak{a} = (f_1, \ldots, f_s) \subseteq \mathbb{Q}(\alpha)[X_1, \ldots, X_n]$, we can assume that the chosen generators are primitive and are in $\mathbb{Z}[\alpha][X, Y, Z]$; we define $\tilde{\mathfrak{a}} = (\tilde{f_1}, \ldots, \tilde{f_s}) \subseteq R_p$.

Remark 4.2.3. *Observe that the definition of $\tilde{\mathfrak{a}}$ is independent on the chosen set of generators of $\mathfrak{a}$, that is*

$$\textit{if } \mathfrak{a} = (f_1, \ldots, f_s) = (f'_1, \ldots, f'_l) \quad \textit{then} \quad (\tilde{f_1}, \ldots, \tilde{f_s}) = (\tilde{f'_1}, \ldots, \tilde{f'_l})$$

as ideals in R_p.

Example 4.2.4. *Consider the ideal*

$$\mathfrak{a} = (3\,Y^2 - 2\,\sqrt{3}ZX, 3\,YX - \sqrt{3}\sqrt{2}Z, 2\,X^2 - \sqrt{2}Y).$$

This set of generators has coefficients in the algebraic extension $\mathbb{Q}(\sqrt{2} + \sqrt{3})$, which is normal, $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = 4$, the minimal polynomial of $\sqrt{2}+\sqrt{3}$ is $q(T) = T^4 - 10T^2 + 1$.

Consider now $p = 23$:

$$q(T) = (T + 21) \cdot (T + 12) \cdot (T + 2) \cdot (T + 11) \mod p.$$

We consider the homomorphism ψ_p such that $\psi_p(\sqrt{2} + \sqrt{3}) = 21$. With this definition of ψ_p, we have that: $\psi_p(\sqrt{2}\sqrt{3}) = 11, \psi_p(\sqrt{2}) = 5, \psi_p(\sqrt{3}) = 16$.
So $\tilde{\mathfrak{a}} = (3\,Y^2 + 14\,ZX, 3\,YX + 12\,Z, 2\,X^2 + 18\,Y)$.

In order to compare $\mathfrak{a}$ and $\tilde{\mathfrak{a}}$, we fix a term order, we compute a Groebner Basis of $\mathfrak{a}$ in $\mathbb{Q}(\alpha)[X_1, \ldots, X_n]$, $\{g_1, \ldots, g_r\}$, with respect to σ. We multiply each g_i with a scalar c_i such that $c_i \cdot g_i \in \mathbb{Z}[\alpha][X_1, \ldots, X_n]$ and $c_i \cdot g_i$ is primitive. We keep on writing g_i for $c_i \cdot g_i$ and we define $\tilde{\mathfrak{a}}$ using this system of generators: $\tilde{\mathfrak{a}} := (\tilde{g}_1, \ldots, \tilde{g}_s) \subseteq R_p$.

Actually, from now on, when we consider a set of generators of an ideal, we assume that the generators have integer coefficients and are primitive.

Definition 4.2.5. *We say that the integer prime p gives a* good reduction *of the ideal $\mathfrak{a}$ if the affine Hilbert function of $\mathfrak{a}$ is the same as the affine Hilbert function of $\tilde{\mathfrak{a}}$.*

Theorem 4.2.2 gives a necessary condition for a prime integer p to preserve the affine Hilbert function of $\mathfrak{a}$: if p preserves $HF^a_{R/\mathfrak{a}}$ then p also preserves $LM_\sigma(\mathfrak{a})$ with respect to a degree-compatible term order σ.

We will show that a finite number of primes p does not satisfy a necessary condition.

Lemma 4.2.6. *Consider α algebraic number on $\mathbb{Q}$, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = s$, $L_1, \ldots, L_N$ non-zero elements of $\mathbb{Z}[\alpha]$, $L_i = \sum_{j=0}^{s-1} a_j^{(i)} \alpha^j$. There is a finite number of prime integers p such that $\psi_p(L_i) = 0$ for some i.*

Proof. We will proceed by contradiction.

Suppose that there are infinite prime integers p such that ψ_p maps to zero one or more of the L_i's. In particular there is an index $\tilde{\imath}$ such that $L_{\tilde{\imath}}$ is mapped to zero by infinite maps ψ_p. Denote $L_{\tilde{\imath}}$ with $\tilde{L}$. We can define the polynomial $\tilde{L}(T) = \sum_{j=0}^{s-1} a_j^{(\tilde{\imath})} T^j$.

If $\deg \tilde{L}(T) = 0$, then we have a contradiction: there is only a finite number of ψ_p mapping the constant $\tilde{L}$ to zero, because there is only a finite number of p's dividing it.

If $d = \deg \tilde{L}(T) \geq 1$, we can consider a prime p such that $\psi_p(\tilde{L}) = 0$ and $p \geq \|\tilde{L}(T)\|^s \|q(T)\|^d$, where $q(T)$ minimal polynomial of α; we can choose such a p since the set of p's we are looking at is supposed to be infinite. But: $\psi_p(\tilde{L}) = \tilde{L}(\beta_p) \mod p = 0$. This means that both $\tilde{L}(T)$ and $q(T)$ can be divided by $(T - \beta_p)$ modulo p. But since $p \geq \|\tilde{L}(T)\|^s \|q(T)\|^d$, $\deg\Big(\gcd(\tilde{L}(T), q(T))\Big) \geq 1$ (applying Lemma 1.4.10). Since $\deg \tilde{L}(T) < \deg q(T)$, this contradicts the fact that $q(T)$ is irreducible. □

Lemma 4.2.7. *Let $\mathfrak{a}$ be an ideal in $\mathbb{Q}(\alpha)[X_1, \ldots, X_n]$, σ a term order and $G = \{g_1, \ldots, g_r\}$ a Groebner Basis of $\mathfrak{a}$ with respect to σ.*
If ψ_p does not map to 0 any of the leading coefficients of the polynomials in G, then $\tilde{G} = \{\tilde{g}_1, \ldots, \tilde{g}_r\}$ is a Groebner Basis of $\tilde{\mathfrak{a}}$ with respect to σ.

Proof. Since G is a system of generators for the ideal $\mathfrak{a}$, then $\tilde{G}$ is a system of generators for $\tilde{\mathfrak{a}}$.

Consider $g \in \mathfrak{a}$ and its representation with respect to the basis G (eventually multiplying for $c \in \mathbb{Z}$, to eliminate the denominators):

$$g = \sum_{i=1}^{r} a_i g_i, \quad a_i \in R.$$

Then we have the corresponding representation of $\tilde{g}$ with respect to the basis $\tilde{G}$:

$$\tilde{g} = \sum_{i=1}^{r} \tilde{a}_i \tilde{g}_i.$$

We have that $LM(\tilde{g}) = \max_{i=1,\dots,r}\{LM(\tilde{a}_i\tilde{g}_i)\}$, where the max is taken with respect to σ.

Since $LM(\tilde{a}_i\tilde{g}_i) = LM(\tilde{a}_i)LM(\tilde{g}_i)$ for every i and ψ_p does not map to zero the leading coefficients of the polynomials in the Groebner basis, we immediately have $LM(\tilde{g}) \in (LM(\tilde{g}_1), \dots, LM(\tilde{g}_s))$ and so $\tilde{G}$ is a Groebner Basis for $\tilde{\mathfrak{a}}$. □

Theorem 4.2.8. *Let $\mathfrak{a}$ be an ideal in $R = \mathbb{Q}(\alpha)[X_1, \dots, X_n]$. Then for a finite number of prime integers p, we have that*

$$HF^a_{R/\mathfrak{a}}(i) \neq HF^a_{R_p/\tilde{\mathfrak{a}}}(i) \quad \textit{for some } i.$$

Proof. We fix a degree compatible term order σ and consider the Groebner Basis $G = \{g_1, \dots, , g_r\}$ of $\mathfrak{a}$. Thanks to Proposition 4.2.1, if $LM(\mathfrak{a}) \neq LM(\tilde{\mathfrak{a}})$ then $HF^a_{R/\mathfrak{a}} \neq HF^a_{R_p/\tilde{\mathfrak{a}}}$. We apply Lemma 4.2.7: there is only a finite number of primes p such that the initial ideals of $\mathfrak{a}$ and $\tilde{\mathfrak{a}}$ are different. □

Corollary 4.2.9. *There is a finite number of prime integers p such that* $\dim \mathfrak{a} \neq \dim \tilde{\mathfrak{a}}$.

4.3 Modular Algorithms

We use the results of Section 4.2 on the exact strategy of decomposition presented in Section 4.1. We develop an algorithm which given an ideal of $\mathbb{Q}[X, Y, Z]$ defining a curve $\mathscr{C}$ in $\mathbb{C}^3$, gives back the number of irreducible components, their degrees, their multiplicities, the algebraic extension in which the non-rational components are defined and the affine Hilbert functions of the components of multiplicity 1.

Remark 4.3.1. *In Step 7 of Algorithm 10 we wrote down the modular factorization grouping together the modular factors D_{ij} corresponding to a rational factor d_i. This is not really necessary for the execution of the algorithm, but it is possible looking at the multiplicities and degrees and in case of ambiguities, computing also the rational factorization of $D_2(x_0, Y)$ and using Algorithm 8.*

Algorithm 8 Partition of modular factors

Input: $d(Z)$ rational factor of $D(x_0, Z)$, an integer p and $D(X, Z) = \prod_{i=1}^{l} D_i(X, Z)^{m_i} \mod p$.

Output: M set of modular factors corresponding to $d(Z)$.

$M :=$ empty list, $i := 1$, $\delta := 1$
while $i \leq l$ **do**
  if $m_i =$ multiplicity of $d(Z)$ in the rational factorization of $D(X, Z)$ **then**
    if $D_i(x_0, Z) \mod p$ divides $d(Z) \mod p$ **then**
      add $D_i(X, Z)$ to M
      $\delta = \delta \cdot D_i(x_0, Z) \mod p$
      if $\delta = d(Z) \mod p$ **then**
        $i := l + 1$
      end if
    end if
  end if
  $i := i + 1$
end while
return M

Algorithm 9 Matching of modular factors through affine Hilbert Dimension

Input: $D_{ij}^{(1)}(X, Z)$ modular factor of $D_1(X, Z)$ and $\{D_k^{(2)}(X, Y) \mod p\}_{k=1,\ldots,m}$ modular factors of $D_2(X, Z)$.

Output: $\tilde{\mathfrak{a}}_{i1} = (F, G, D_{i1}^{(1)}(X, Z)^{m_i}, D_{i1}^{(2)}(X, Z)^{m_i}) \mod p$ with Hilbert dimension 1

$k := 1$
while $k \leq m$ **do**
  if $\deg(D_k^{(2)}(x_0, Y)) = \deg(D_{ij}^{(1)}(x_0, Z))$ **then**
    if Hilbert Dimension of $(F(x_0, Y, Z), G(x_0, Y, Z), D_{ij}^{(1)}(x_0, Z)^{m_i}, D_k^{(2)}(x_0, Z)^{m_k}) \mod p$ is 0 **then**
      renumber the modular factor putting $D_{i1}^{(2)}(X, Y) := D_k^{(2)}(X, Y)$
      $k := m + 1$
    else
      $k := k + 1$
    end if
  end if
end while
return $\tilde{\mathfrak{a}}_{i1} = (F, G, D_{i1}^{(1)}(X, Z)^{m_i}, D_{i1}^{(2)}(X, Z)^{m_i}) \mod p$.

Algorithm 10 Modular Algorithm for affine Hilbert Function

Input: $\mathfrak{a} = (F, G) \in \mathbb{Q}[X, Y, Z]$, $Z \subseteq \mathbb{Z}$ finite set.

Output: The degree and multiplicity of at least one irreducible component $\mathscr{C}_1$ of the curve $V(\mathfrak{a})$, the number of conjugates component and if $\mathscr{C}_1$ has multiplicity 1, its affine Hilbert function.

1: **Preprocessing:** Perform a generic integer change of coordinates on F and G, with coefficients in $\mathbb{Z}$; choose $(x_0, y_0, z_0) \in \mathbb{Z}^3$.
2: Compute $D_1(x_0, Z) := Res_Z(F(x_0, Y, Z), G(x_0, Y, Z))$ and $D_2(x_0, Y) := Res_Y(F(x_0, Y, Z), G(x_0, Y, Z))$
3: Compute the rational factorization:$D_1(x_0, Z) = d_1^{(1)}(Z)^{m_1} \cdots d_s^{(1)}(Z)^{m_s}$
4: **for** i from 1 to s **do**
5: Choose a prime integer p dividing $d_i^{(1)}(x_0, z_0)$.
6: Compute $D_1(X, Z) := Res_Y(F, G) \mod p$ and $D_2(X, Y) := Res_Z(F, G) \mod p$
7: Compute the modular factorizations:

$$D_k = \left(\prod_{j=1}^{r_1} D_{1j}^{(k)}\right)^{m_1} \cdots \left(\prod_{j=1}^{r_s} D_{sj}^{(k)}\right)^{m_s} \mod p, \quad k = 1, 2$$

8: Apply Algorithm 9 to the rational factor $d_i^{(1)}(Z)$ and the modular factors of $D_1(X, Z)$, obtaining the set of modular factors $D^{(1)}$ of $D_1(X, Z)$and to the rational factor $d_i^{(2)}(Z)$ and the modular factors of $D_2(X, Y)$, obtaining the set of modular factors $D^{(2)}$of $D_2(X, Y)$.
9: **if** $r_i \geq 2$ **then**
10: Choose $D_{ij}^{(1)}(X, Z) \mod p \in D^{(1)}$ of minimal degree such that $r_i = \frac{\deg d_i^{(1)}(Z)}{\deg D_{ij}^{(1)}(X,Z)} \in \mathbb{Z}$ $(*)$
11: Consider $D_{ij}^{(1)}(X, Z)$ and compute the polynomial defining $\mathbb{Q}(\alpha_i)$ using Proposition 1.4.11 with $Q = \|F\|^{d_2}\|G\|^{d_1}$, $s = r_i$
12: Apply Algorithm 9 to match the modular factor $D_{ij}^{(1)}(X, Z)$ with a modular factor of $D_2(X, Y)$ obtaining $\tilde{\mathfrak{a}}_{i1} = (F, G, D_{i1}^{(1)}(X, Z)^{m_i}, D_{i1}^{(2)}(X, Z)^{m_i}) \mod p$ (after re-labelling of the factors)
13: **if** m_i is 1 **then**
14: Compute the Jacobian matrix of $(F, G) \mod p$ and a minor of size 2×2, $\tilde{S}$.
15: Compute $\tilde{\mathfrak{a}}_i^{(\tilde{S})}$ the saturation of $\tilde{\mathfrak{a}}_i$ with respect to $\tilde{S}$.
16: **end if**
17: **end if**
18: **end for**
19: **return** s number of rational components
for every $i = 1, \ldots, s$: r_i number of non-rational components in $\mathscr{C}_i$, $\deg D_{ij}^{(1)}(X, Z)$ degree of the non-rational component, m_i multiplicity of the non-rational component;
if $m_i = 1$, p and $\tilde{\mathfrak{a}}_i^{(\tilde{S})} \mod p$ ideal modulo p of a non-rational component of $\mathscr{C}_i$ having the same Hilbert function as $I(\mathscr{C}_i)$; if $m_i \geq 2$ p and $D_{i1}^{(1)}(X, Z)^{m_i}, D_{i1}^{(2)}(X, Z)^{m_i}$ image modulo p of 2 separator polynomials for $\mathscr{C}_i$

Remark 4.3.2. *We did not present a non-modular version of Algorithm 8, since all the algorithms presented in Section 4.1.1 are not actually used. We insert this further procedure to avoid useless computations in the calling of Algorithm 9 in Step 8 of Algorithm 10.*
In order to speed up the computations in Algorithm 9, we use the fact that a generic plane section of a finite set of points in $\mathbb{C}^3$ is empty. We also assume that the Hilbert dimension of the empty set is -1.

4.3.1 Proof of Algorithm 10

We can apply the results of Section 4.2 to the decomposition strategy explained in Section 4.1 and the Algorithms of Section 4.1.1 and adapt them to modular computations. Again, we deal with an ideal $\mathfrak{a} = (F, G) \subseteq \mathbb{Q}[X, Y, Z]$ defining a curve $\mathscr{C} = V(\mathfrak{a})$. For all the notations used, we refer to Algorithms 8, 9 and 10.

In Step 1, as in Algorithm 6, we perform a generic change of coordinates; thanks to this, two projections on the coordinate planes are "generic" in the sense of Proposition 4.1.2: the components of projected curve are in one-to-one correspondence with the components of the curve itself (see also Corollary 4.1.3). Furthermore, consider the factors of the polynomial whose set of zeroes is the projected curve and the primary components of the ideal defining the curve: factors and primary components are in one-to-one correspondence and the degree and multiplicity of one factor is the degree and multiplicity of the corresponding primary component (in the sense of Definition 2.1.14 and 2.1.15).

In order to apply the modular techniques for absolute decomposition of polynomials developed in Chapter 1, we have to be careful because we do not have one hypothesis: the Input of Algorithm 4 is a *rationally irreducible* polynomial. This is not our situation.
Indeed, assume that we are able to compute $D_1(X, Z) = Res_Y(F, G)$. This bivariate polynomial in general is not rationally irreducible; furthermore it is not advantageous to compute the bivariate rational factorization of D_1.
We rely on Hilbert's Irreducibility Theorem (Theorem 1.2.3): for infinite integer specialization of one variable, a rationally irreducible factor of the polynomial D_1 stays rationally irreducible. This means that if

$$D_1(X, Z) = d_1^{(1)}(X, Z)^{m_1} \cdots d_s^{(1)}(X, Z)^{m_s} \in \mathbb{Q}[X, Z]$$

then for infinite $x_0 \in \mathbb{Z}$ the rational factorization of $D_1(x_0, Z)$ is exactly

$$D_1(x_0, Z) = d_1^{(1)}(x_0, Z)^{m_1} \cdots d_s^{(1)}(x_0, Z)^{m_s} \in \mathbb{Q}[Z].$$

In order to compute this rational univariate factorization without the computational effort of computing $D_1(X, Z)$, in Step 2 we simply specialize one variable of F and G and then

compute the resultant:

$$Res_Y(F(x_0, Y, Z), G(x_0, Y, Z)) = D_1(x_0, Z).$$

Since we are considering a generic projection, a rational factor $d_i^{(1)}(X, Z)$ of $D_1(X, Z)$ corresponds to a rational component of the curve (in the sense of Definition 2.2.2), while each absolute factor of $d_i^{(1)}(X, Z)$ corresponds to an irreducible component.

Once computed in Step 3 the univariate rational factorization, we then proceed in order to "break" the non-rational components.
We consider the i-th factor of the rational factorization of $D_1(x_0, Z)$, that is $d_i^{(1)}(Z)$ which has multiplicity m_i. If the corresponding factor $d_i^{(1)}(X, Z)$ of the bivariate rational factorization of $D_1(X, Z)$ is not absolutely irreducible, then its absolute factors have coefficients in some algebraic extension $\mathbb{Q}(\alpha_i)$. Using Lemma 1.4.1, we can assume that the algebraic extension $\mathbb{Q}(\alpha_i)$ is generically generated by the evaluation of one absolute factor in an integer point, $(x_0, z_0) \in \mathbb{Z}^2$.
We choose an integer prime p dividing $d_i(z_0)$ (Step 5). We rely on randomness in order to avoid a p giving a bad reduction of $d_i^{(1)}(X, Z)$ (and of $D_1(X, Z)$). If the chosen p is big enough we can rely on Lemma 1.4.9: this means that if we factor $D_1(X, Z)$ modulo this prime p, the rationally irreducible factor $d_i^{(1)}(X, Z)$ splits (if it is not absolutely irreducible). The homomorphism ψ_p of (4.2.1) is implicitly defined.
Actually we do not compute $D_1(X, Z)$ nor $D_2(X, Y)$: in fact, in Step 6 we compute directly the modular resultants $Res_Y(F, G) \mod p$ and $Res_Z(F, G) \mod p$ and then the modular factorizations (Step 7).

If the rational factor $d_i^{(1)}(X, Z)$ is absolutely irreducible, then the corresponding modular factor is simply $D_{i1}^{(1)}(X, Z)^{m_1} \mod p$, that is $r_i = 1$. In this case, we can stop here and repeat this part of the process for the next rational factor.
If $d_i^{(1)}(X, Z)$ is absolutely reducible, then $r_i \geq 2$ (thanks to the choice of p according to Lemma 1.4.9): in Step 8 we group the modular factors corresponding to $d_i^{(1)}(Z)$ and we choose a modular factor among them having minimal degree which divides $\deg d_i^{(1)}(Z)$; we assume that this factor is $D_{i1}^{(1)}(X, Z)$.
In Step 12 we look for the corresponding modular factor of D_2, $D_{ij}^{(2)}(X, Y)$, using Algorithm 9, obtaining the ideal $\tilde{\mathfrak{a}}_{i1} = (F, G, D_{i1}^{(1)}(X, Z), D_{i1}^{(2)}(X, Y)) \mod p$ with Hilbert dimension 1. Corollary 4.2.9 certifies that $\tilde{\mathfrak{a}}_{i1} = \psi(\mathfrak{a}_{i1})$, where $\mathfrak{a}_{i1} = (F, G, D_{i1}^{(1)}(X, Z), D_{i1}^{(2)}(X, Y))$ is the ideal in (4.1.3).

Furthermore, just like in Algorithm 4, Step 13, in Step 11 we can use the techniques of Section 1.4.3. In particular, we can apply Proposition 1.4.11 using $Q \geq \|Res_Z(F, G)\| \geq \|F\|^{\deg(G)}\|G\|^{\deg(F)}$. The degree of the polynomial we wish to construct is $s_i = \frac{\deg d_i(Z)}{\deg D_{i1}^{(1)}}$. It is not necessary to lift the whole modular factorization of $D_1(X, Z)$ modulo p in order to

have the p-adic approximation of α to the desired degree of accuracy. It is sufficient to lift the modular factorization $d_i(Z) = D_{i1}^{(1)}(x_0, Z) \cdot \left(\prod_{j=2}^{r_1} D_{ij}^{(1)}(x_0, Z)\right)$.

Once defined the ideal $\tilde{\mathfrak{a}}_{i1} = (F, G, D_{i1}^{(1)}(X, Z)^{m_i}, D_{i1}^{(2)}(X, Y)^{m_i}) \mod p$ (re-ordering the indexes) with affine Hilbert dimension 1, if the multiplicity m_i is 1, we can keep on following Steps 5 and 6 of Algorithm 6: we compute the Jacobian Matrix of $(F, G) \mod p$ and consider one of its (2×2)-minors, $\tilde{S}$. We compute the colon ideal of $\tilde{\mathfrak{a}}_{i1}$ with $\tilde{S}$, obtaining $\tilde{\mathfrak{a}}_{i1}^{(\tilde{S})}$.

We need to show that for infinite primes p the colon ideal modulo p has the same affine Hilbert function of the colon ideal in $\mathbb{Q}(\alpha)[X, Y, Z]$, that is $\psi_p(\mathfrak{a}_{i1}^{(S)}) = \tilde{\mathfrak{a}}_{i1}^{(\tilde{S})}$ (with $\mathfrak{a}_{i1}^{(S)}$ the ideal of Proposition 4.1.9).
First of all, observe that $\tilde{\mathfrak{a}}_{i1}$ and the corresponding non-modular ideal $\mathfrak{a}_{i1}$ have the same Hilbert function for all but a finite number of integers p (thanks to Theorem 4.2.8).
Furthermore, we can assume that we compute Jacobian matrix of $\mathfrak{a}$ and a minor S and then reduce modulo p. For what concerns the colon ideal, the actual computation is performed using a Groebner Basis (see Section 4.4.1 for the details). This means that again we can apply Lemma 4.2.7 and so there is only a finite number of prime p such that $\psi_p(\mathfrak{a}_{11}^{(S)})$ and $\tilde{\mathfrak{a}}_{11}^{(S)}$ differ.

Remark 4.3.3. *Actually, Algorithm 10 is a Las-Vegas one, just like Algorithm 4: in fact, in the Preprocessing Step, we have to assume that the coefficients for the generic change of coordinates are taken in a finite set $S_1 \in \mathbb{Z}$ and the point (x_0, y_0, z_0) is in S_2^3, $S_2 \subseteq \mathbb{Z}$ finite set.*
With this assumption, we have to modify the Preprocessing Step of Algorithm 10:

> ***Preprocessing:*** *Perform a generic integer change of coordinates on F and G, with coefficients in S_1 finite subset of $\mathbb{Z}$; choose $(x_0, y_0, z_0) \in S_2^3$, S_2 finite subset of $\mathbb{Z}^3$.*

Furthermore, we have to insert the following small loop in Step 10:

> ***if*** $\deg \tilde{D}_1 \neq (\deg F) \cdot (\deg G)$ ***or*** $\deg \tilde{D}_2 \neq (\deg F) \cdot (\deg G)$ ***then***
> ***if*** *not all primes dividing $d_i(z_0)$ have already been used* ***then***
> *go back to Step 5 and change p*
> ***else***
> *go back to the Preprocessing Step*
> ***end if***
> ***end if***

If all the integers in S_1 and S_2 are used without ending the Algorithm, then the Algorithm returns "I can not compute the irreducible components".

4.3.2 Tricks on an example

Consider the complete intersection ideal $\mathfrak{a} = (F, G)$ with

$$
\begin{aligned}
F:=&-2566702905942050\,X^4Z^4+459256557993984\,X^2Y^4Z^2-43055302311936\,X^2Y^3Z^3+149908695810048\,X^2Y^2Z^4+\\
&-6979668148224\,X^2YZ^5+6071229709824\,X^2Z^6-3503849472\,Z^8-42050955749032480\,X^4Z^3+\\
&-10266811623768200\,X^3Z^4+7348104927903744\,X^2Y^4Z-803698976489472\,X^2Y^3Z^2+3607675539554304\,X^2Y^2Z^3+\\
&-186713130663936\,X^2YZ^4+195165738909696\,X^2Z^5+918513115987968\,XY^4Z^2-86110604623872\,XY^3Z^3+\\
&+299817391620096\,XY^2Z^4-13959336296448\,XYZ^5+12142459419648\,XZ^6-168184774656\,Z^7+\\
&-153165621418742832\,X^4Z^2-168203822996129920\,X^3Z^3+29392419711614976\,X^2Y^4-1294770487689216\,X^2Y^3Z+\\
&+28848282705543168\,X^2Y^2Z^2-2969746688299904\,X^2YZ^3-14335675247912668\,X^2Z^4+14696209855807488\,XY^4Z+\\
&-1607397952978944\,XY^3Z^2+7215351079108608\,XY^2Z^3-373426261327872\,XYZ^4+390331477819392\,XZ^5+\\
&+459256557993984\,Y^4Z^2-43055302311936\,Y^3Z^3+169137821712384\,Y^2Z^4-9871924445184\,YZ^5+\\
&+4283168847360\,Z^6+156192183008469632\,X^4Z-612662485674971328\,X^3Z^2+19034255810101248\,X^2Y^3+\\
&+77148501872836608\,X^2Y^2Z-26269071740640768\,X^2YZ^2-260503407032577912\,X^2Z^3+58784839423229952\,XY^4+\\
&-2589540975378432\,XY^3Z+57696565411086336\,XY^2Z^2-5939493376599808\,XYZ^3-8137727248288936\,XZ^4+\\
&+7348104927903744\,Y^4Z-803698976489472\,Y^3Z^2+4069174561210368\,Y^2Z^3-274458050691072\,YZ^4+\\
&+209669071610880\,Z^5-35411347230556448\,X^4+624768732033878528\,X^3Z-76439088940073148\,X^2Y^2+\\
&-135717859082331792\,X^2YZ-837794589252510608\,X^2Z^2+38068511620202496\,XY^3+154297003745673216\,XY^2Z+\\
&-52538143481281536\,XYZ^2-184599168072895984\,XZ^3+3010058973609984\,Y^4+6641580791169024\,Y^3Z+\\
&+27619879438268416\,Y^2Z^2-3314693704751488\,YZ^3-1290430395206738\,Z^4-141645388922225792\,X^3+\\
&+52319931666594104\,X^2Y+925556148166809200\,X^2Z-152878177880146296\,XY^2-271435718164663584\,XYZ+\\
&-450264207155078560\,XZ^2+69333885671964672\,Y^3+44942962614968320\,Y^2Z-21960926297551616\,YZ^2+\\
&-50543547879625656\,Z^3-209591503386136124\,X^2+104639863333188208\,XY+601574832265861344\,XZ+\\
&-100413940824686780\,Y^2-112229039722104464\,YZ-77719642153201576\,Z^2-135892228927820664\,X+\\
&+52319931666594104\,Y+144595233124461040\,Z-32534767233353884.
\end{aligned}
$$

$$
\begin{aligned}
G:=&12580089921\,X^4Y^2-125947381476\,X^4YZ+315235085764\,X^4Z^2-56061591552\,X^2Y^4+5255774208\,X^2Y^3Z+\\
&-18299401344\,X^2Y^2Z^2+705303684\,X^2YZ^3-738880698\,X^2Z^4+427716\,Z^6-23984732562\,X^4Y+120063301636\,X^4Z+\\
&+50320359684\,X^3Y^2-503789525904\,X^3YZ+1260940343056\,X^3Z^2+14015397888\,X^2Y^3-147599659008\,X^2Y^2Z+\\
&+6812660448\,X^2YZ^2-11930741496\,X^2Z^3-112123183104\,XY^4+10511548416\,XY^3Z-36598802688\,XY^2Z^2+\\
&+1410607368\,XYZ^3-1477761396\,XZ^4+13686912\,Z^5+11432100241\,X^4-95938930248\,X^3Y+\\
&+480253206544\,X^3Z+13588239750\,X^2Y^2-504452464808\,X^2YZ+1838507201030\,X^2Z^2+28030795776\,XY^3+\\
&-295199318016\,XY^2Z+13625320896\,XYZ^2-23861482992\,XZ^3-56061591552\,Y^4+5255774208\,Y^3Z+\\
&-18299401344\,Y^2Z^2+985906308\,YZ^3-579022170\,Z^4+45728400964\,X^3-96421675372\,X^2Y+\\
&+711716717848\,X^2Z-73464239868\,XY^2-1325877808\,XYZ+1155133715948\,XZ^2+14015397888\,Y^3+\\
&-147599659008\,Y^2Z+11302302432\,YZ^2-11124929784\,Z^3+67851322438\,X^2-965490248\,XY+\\
&+462927022608\,XZ-3289947071\,Y^2+141804814796\,YZ+263814330226\,Z^2+44245842948\,X+\\
&+23501987438\,Y+111400209668\,Z+10690821233;
\end{aligned}
$$

The complete intersection curve $\mathscr{C} = V(\mathfrak{a})$ has degree 48.

We perform a generic linear change of coordinates and we compute

$$r := Res_Z(F(0, Y, Z), G(0, Y, Z)),$$

which has degree 48 and factors over the rationals (in less than 1 second) as:

- $d_1^{(1)}(Y)$ factor of degree 8 and multiplicity 1;
- $d_2^{(1)}(Y)$ factor of degree 24 and multiplicity 1;
- $d_3^{(1)}(Y)$ factor of degree 2 and multiplicity 1;
- $d_4^{(1)}(Y)$ factor of degree 14 and multiplicity 1.

So, using Definition 2.2.2, the complete intersection $\mathfrak{a}$ has 4 rational components $\mathfrak{q}_i$, all of multiplicity 1, with degrees given by $\deg d_i^{(1)}(Y)$ (thanks to Corollary 4.1.3).
We then choose $p_1 = 10639$ which divides the constant term of $d_1^{(1)}(Y)$.
The computations of $D_1(X,Z) = Res_Y(F,G) \mod p_1$, $D_2(X,Y) = Res_Z(F,G) \mod p_1$ and their modular factorization take about 10 seconds.
The rational factor of degree 8 further splits modulo p_1 in 2 factors of degree 4 each. Observe that also the other rational factors splits as a product of two modular factors; in particular, we have that the rational factor of degree 14 splits in 2 modular factors of degree 7 each and the rational factor of degree 2 splits in 2 modular factors of degree 1 each. Since the degrees of this modular factors are prime numbers, they can not further split (thanks to Lemma 1.1.4) and we can compute the Hilbert function of these components too without changing the prime p_1.

We can match the factors of degree 4 in the factorizations of $D_1(X,Z)$ and $D_2(X,Y)$ through the Hilbert dimension of a generic plane section and consider the ideals $\tilde{\mathfrak{a}}_i = (F, G, D_i^{(1)}, D_i^{(2)}) \mod p_1, i = 1, 2$.
We then compute a 2×2 minor S of the Jacobian matrix of $\mathfrak{a}$ and compute the quotient ideals

$$\tilde{\mathfrak{a}}_1 : S \mod p_1 \qquad \tilde{\mathfrak{a}}_2 : S \mod p_1$$

and this takes less than 25 seconds. In this way we obtain the Hilbert functions of two irreducible components $\mathscr{C}_1$ and $\mathscr{C}_2$ of $\mathscr{C}$.

The same for the modular factors of degree 7: we match them through the Hilbert function of a generic plane section obtaining $\tilde{\mathfrak{a}}_3, \tilde{\mathfrak{a}}_4$, compute the quotient with respect to S in about 280 seconds (this is due to the higher degree of the generators of $\tilde{\mathfrak{a}}_3, \tilde{\mathfrak{a}}_4$) and get the Hilbert function of the components $\mathscr{C}_3$ and $\mathscr{C}_4$ of $\mathscr{C}$.

Finally, we match the modular factors of degree 1. Since the two matched modular factors of degree 1 completely describe a line, we do not need to define $\tilde{\mathfrak{a}}_5$ and $\tilde{\mathfrak{a}}_6$ and then saturate, it is sufficient to directly consider the two ideals defined by the matched couples of factors.

The only modular factors left are the ones of degree 12. Since we chose p_1 in order to split the modular factor of degree 8 with at least one linear factor, it is possible that these two factors are of degree higher than the degree of an absolute factor of the rational factor of degree 24.

We can proceed in the following way:

- we choose $p_2 = 967$ dividing the constant term of $d_2^{(1)}(Y)$;
- we compute the resultants modulo p_2 and their modular factorization.

In this case, we have that the rational factor of degree 24 splits in two modular factors of degree 12 each. This means that we can compute the Hilbert function of these non-rational components also modulo p_1, since it gives the correct splitting.

After matching the factors, we can then compute also the two quotients

$$\tilde{\mathfrak{a}_7} : S \mod p_1, \qquad \tilde{\mathfrak{a}_8} : S \mod p_1,$$

obtaining also the Hilbert functions of the two components left, $\mathscr{C}_7$ and $\mathscr{C}_8$.

Finally, using the techniques of Algorithm 4 we can compute the polynomial $M(T)$ defining the algebraic extension $\mathbb{Q}(\alpha)$ where we have a set of generators for any $\mathfrak{q}_i^{(j)}$ of the absolute decomposition of $\mathfrak{a}$:

$$\begin{aligned} M(T) = &- 1108258016301093388576096467370739001050958 4\,T^2 + \\ &+ 1316903182666682902924191848784529278874959 60\,T + \\ &- 2966451789421981811913388875047715693266504 25. \end{aligned}$$

Obviously, since $\deg M(T) = 2$, we can easily find a better presentation of the extension $\mathbb{Q}(\alpha)$ computing the roots of $M(T)$: we obtain that the extension of $\mathbb{Q}$ we need can be generated by $\sqrt{2}$.

Summing up, we obtained that the complete intersection curve $\mathfrak{a} = (F, G) \subseteq \mathbb{Q}[X, Y, Z]$ has the rational primary decomposition

$$\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \mathfrak{q}_3 \cap \mathfrak{q}_4$$

with $\deg \mathfrak{q}_1 = 8$, $\deg \mathfrak{q}_2 = 24$, $\deg \mathfrak{q}_3 = 2$ and $\deg \mathfrak{q}_4 = 14$ and all the primary components of multiplicity one.

Each of the rational primary ideals further decomposes as

$$\mathfrak{q}_i = \mathfrak{q}_i^{(1)} \cap \mathfrak{q}_i^{(2)},$$

with $\mathfrak{q}_i^{(j)} \subseteq \mathbb{Q}(\sqrt{2})[X, Y, Z]$, $\mathfrak{q}_i^{(2)} = \sigma\left(\mathfrak{q}_i^{(1)}\right)$, where $\sigma(\sqrt{2}) = \sqrt{2}$.

Using the Maple command `PrimaryDecomposition` (whose algorithm is based on [32]), we could not obtain the primary decomposition of $\mathfrak{a}$ over the rationals: the memory allocation failed (reaching more than 2.5 GB) after more than 2 hours of computations. This Maple command can also give a primary decomposition using as coefficient field an algebraic extension of the rationals, but one needs to know a priori which is the right extension in which the primary components further split. Even with this further information about

the decomposition, `PrimaryDecomposition` in Maple caused a problem with memory allocation (reaching about 2.3 GB), after computing for more than 1 hour.

We used Singular ([36]), another computer algebra system for polynomial computations. We tried to obtain the rational primary decomposition of $\mathfrak{a}$ using `primdecGTZ` and the primary decomposition over $\overline{\mathbb{Q}}[X,Y,Z]$ using `absprimdecGTZ` (which are based on [32], the algorithms are described in [22]). In both cases we stopped the computations after 2 hours, without obtaining the primary decomposition.

We would like to compare our results (from the point of view of the obtained information and timings) with another library, Jean-Charles Faugere's $F7$, but we could not find either a distribution or an exhausting documentation on it.

4.4 Other modular strategies

The algorithms of Section 4.3 are a sort of "black box" which predicts the Hilbert function of the reduced and irreducible components of the curve defined by the ideal $\mathfrak{a} = (F,G) \subseteq \mathbb{Q}[X,Y,Z]$. From this, we can immediately obtain a bound on the degree of a separator polynomial for each component and use it to reduce the computations of a numerical algorithm of decomposition.

After applying Algorithm 10 to the ideal $\mathfrak{a}$, we obtain for each rational primary component $\mathfrak{q}_i$:

$$P_i \in \mathbb{Z}/p\mathbb{Z}[X,Y,Z], P_i \in \mathfrak{q}_i \mod p,$$

and $\overline{P}_i \in (\mathfrak{a} : \mathfrak{q}_i)$ such that

$$P_i\overline{P}_i \mod p \in \mathfrak{a} \mod p, \quad P_i, \overline{P}_i \notin \mathfrak{a} \mod p,$$

that is

$$(P_i\overline{P}_i = \eta F + \mu G) \mod p. \tag{4.4.1}$$

If $\mathfrak{q}_i$ is a rational component of $\mathfrak{a}$ of multiplicity 1, then we can choose $P_i \mod p$ of minimal degree among the generators of $\mathfrak{q}_i \mod p$; if the multiplicity of $\mathfrak{q}_i$ is ≥ 2, then we will take $P_i = D_{i1}^{(1)}(X,Z) \mod p$.

Can we reconstruct from the polynomial $P_i \mod p$ and from (4.4.1), a separator polynomial for each rational component of $\mathfrak{a}$? In other words, can we lift modulo p an ideal (or at least a polynomial of an ideal) and then recognize the rational coefficients from their p-adic approximations?

The last part of this question is the only one which has a complete answer: if we have a positive integer N bounding the size of the numerators and of the denominators of the coefficients of the separator polynomials, then we can use the recognition of Farey fractions

to reconstruct the rational from its p-adic approximation (see Section B.6). The bound N allows us to choose the appropriate level of p-adic approximation λ to recognize the rational we look for among the possible rational numbers which have the same first λ p-adic digits. So, if we were able to lift a polynomial which is in a given ideal, we would be done.

Actually we can look at this problem of lifting arising from the computation modulo p of the Hilbert function of the irreducible and reduced components of a curve of $\mathbb{C}^3$, as a generalization of the Hensel lifting for a univariate factorization.
Obviously, one may think to generalize the Hensel step (Algorithm 14) to the modular factorization of a multivariate polynomial: geometrically, it is equivalent to keep on working with objects of codimension 1, but in an affine space of higher dimension. Our point of view, is instead to keep on working on objects of small dimension (1, not 0 as in the case of univariate polynomials) in an affine space of higher dimension.

It is not possible to directly apply the same arguments and construction of the Hensel Step, simply because we do not have an algebraic hypothesis which is absolutely necessary in the univariate lifting: the two modular univariate factors are coprime (that is, by means of Euclidean division we have a Bezout's identity of kind $su + tv \equiv 1 \mod p$). Even if we fix a term order generalizing the Euclidean division to multivariate polynomials, we do not have a Bezout's identity of kind $sP_1 + t\overline{P}_1 \equiv 1 \mod p$, since in general the ideal $(F, G, P_1, \overline{P}_1) \mod p$ is not (1).

4.4.1 An exact modular strategy

The problem of lifting p-adically a polynomial was already investigated in a particular setting: since modular computations are faster, it is convenient to pass from computations on the rational numbers to computations modulo p to obtain a Groebner Basis.

The basic idea is: during the execution of Buchberger algorithm, many S-polynomials are computed before reaching the Groebner Basis and the coefficients of these intermediate polynomials may grow to enormous size; we can then perform Buchberger algorithm using modular arithmetic for a well-chosen prime p, and then lift the reduced (and so unique) modular Groebner Basis to the rational one.

In [1], the investigation of [82] and [64] has been carried on: in [82] for the first time there was the computation of a Groebner Basis passing through modular computations, but assuming that we could choose a priori a "lucky prime" p; in [64] the notion of "lucky prime" is more clearly investigated.
In [1], the author gives some characterizations of "lucky prime" for a rational ideal $\mathfrak{a} = (f_1, \ldots, f_m)$ in $\mathbb{Q}[X_1, \ldots, X_n]$ and a method to distinguish a lucky prime from an unlucky one. So, even if probabilistically, a lucky prime can be chosen. After this, the reduced modular Groebner Basis of $\mathfrak{a}$ is computed. Finally, the author describes a method to lift this

reduced modular basis.
This method bears similarities with the Hensel lifting, in the sense that it works on a modular information (the Groebner Basis) and a rational one (the set of generators $\{f_1, \ldots, f_m\}$ of $\mathfrak{a}$), as in the Hensel lifting we know on the one hand the modular factors and on the other one the rational polynomial.
If a bound on the size of the numerators and denominators of the rational coefficients of the Groebner Basis is known, then it can be used to choose the level of lifting; finally Farey fractions recognition (Algorithm 15) gives the rational coefficients needed. This method can be used in our problem, combining it with the absolute factorization algorithm of Chapter 1. In fact, we can follow Algorithm 6 until Step 3, computing the absolute bivariate factorization of $D_1 = Res_Y(F, G)$ and $D_2 = Res_Z(F, G)$ and the algebraic extensions of $\mathbb{Q}$ involved. If we multiply again the absolute factors in order to have the rational factorizations, we can match the rational factors through Algorithm 7. Then, for any rational component of $\mathfrak{a}$ of multiplicity one, we would like to compute

$$\left((F, G, D_i^{(1)}, D_i^{(2)}) : S\right), \tag{4.4.2}$$

where S is a 2×2 minor of the Jacobian matrix of $\mathfrak{a}$. For this computations (which is a Groebner Basis, as pointed out in the proof of Algorithm 10), we can use the modular techniques of [1]. But actually with a small change, we can use the technique of lifting in a more convenient way for the computation of the quotient ideal.

In general, if we consider an ideal $\mathfrak{a} \subseteq \mathbb{Q}[X_1, \ldots, X_N]$ and $M \in \mathbb{Q}[X_1, \ldots, X_N]$, the standard technique to compute the quotient ideal $(\mathfrak{a} : M)$ is to bring the problem back to the computation of an intersection, since

$$M(\mathfrak{a} : M) = \mathfrak{a} \cap (M),$$

(as proved in [19], Chapter 4, Section 4, Theorem 11). The computation of an intersection of ideals is again performed using a Groebner Basis: if $\mathfrak{a} = (f_1, \ldots, f_r)$, then

$$\mathfrak{a} \cap M = (tf_1, \ldots, tf_r, (1-t)M) \cap \mathbb{Q}[X_1, \ldots, X_N].$$

If we use the technique of [1], we then compute the reduced modular Groebner Basis using an elimination order for the variable t of an ideal in $N + 1$ variables, and then lift it to the rationals.
Both the term order and the number of variables are not advantageous, so we will proceed in a different way.

Assuming that we have chosen a lucky prime p, we compute the reduced modular Groebner Basis of $(tf_1, \ldots, tf_r, (1-t)M)$ with an elimination term order for t; we obtain

$$(MG_1, \ldots, MG_s, \text{ polynomials containing t }) \mod p.$$

Then, we consider the ideal $(MG_1, \ldots, MG_s) \mod p$ and we compute its reduced modular Groebner Basis with respect to a term order more convenient for the computations (for instance, DegRevLex), obtaining the modular Groebner Basis MG_p. We write MG_p since the polynomials in the basis have the form MG; we keep on writing $G_p = \{G_1, \ldots, G_s\}$. We can apply the lifting technique of [1], Section 6.2, keeping track of the fact that the Groebner Basis we look for will be of kind $(Mg_1, \ldots, Mg_s)$.

In the following Algorithm we use the matrix notation of [1], where F is the matrix whose columns are the generators of $\mathfrak{a}$ and G_p is the matrix whose columns are the polynomials in the reduced modular Groebner Basis G_p.

Algorithm 11 Lifting modular Groebner Basis for a quotient ideal

Input: $\mathfrak{a} = (f_1, \ldots, f_r) \subseteq \mathbb{Q}[X_1, \ldots, X_N]$, MG_p modular Groebner Basis of $M(\mathfrak{a} : M)$ with respect to a term order σ, A bound on the size of the numerators and denominators of the rational Groebner Basis of $(\mathfrak{a} : M)$.

Output: $G = (g_1, \ldots, g_s)$ rational reduced Groebner Basis of $(\mathfrak{a} : M)$

1: $i := 2$, $G^{(1)} := G_p$, $\Lambda^{(1)}$ such that $MG_p = \Lambda^{(1)}F \mod p$,
2: **while** $p^i \leq A$ **do**
3: $\quad G' = \dfrac{1}{p^{i-1}}\left(\dfrac{\Lambda^{(i-1)}F}{M} - G^{(i-1)}\right)$
4: $\quad \Lambda' = \mathbf{0}$
5: $\quad$ Reduce G' with respect to $G^{(1)}$: $G' = \Gamma G^{(1)} + G''$
6: $\quad G^{(i)} = G^{(i-1)} + p^i G''$, $\Lambda^{(i)} = \Lambda^{(i-1)} - \Gamma\Lambda^{(1)}$
7: $\quad i := i + 1$
8: **end while**
9: Use Algorithm 15 to reconstruct the rational coefficients of G from $G^{(i)}$
10: **return** G reduced rational Groebner Basis of $(\mathfrak{a} : M)$.

Proof of Algorithm 11. We simply observe that at each recursion of Steps 3-7 we want to have $G^{(i)}$ and $\Lambda^{(i)}$ such that

$$MG^{(i)} \equiv \Lambda^{(i)}F \mod p^i, \tag{4.4.3}$$

and $G^{(i)}$ is a reduced Groebner Basis.

It is straightforward to verify that congruence (4.4.3) is satisfied by $G^{(i)}$ and $\Lambda^{(i)}$ constructed at each recursion. Furthermore $G^{(i)}$ is the reduced Groebner Basis of $(\mathfrak{a} : M)$ modulo p^i thanks to the reduction in Step 5.

Finally, given the bound A, we can use the algorithm for the recognition of Farey fraction (Algorithm 15). □

We can then adapt Algorithm 6 in another way: after computing the resultants in Step 2, we can use an algorithm of bivariate rational factorization and then Algorithm 4 to obtain

the absolute factorization of the resultant; then we can compute the quotient ideal in Step 6 of Algorithm 6 using Algorithm 11.

4.4.2 Lifting Ideals

In Section 4.4.1 we show how an efficient bivariate factorization algorithm and modular computations on Groebner Basis can construct separator polynomials of minimal degree (in the sense that we can choose in (4.4.2) $D_i^{(1)}$ and $D_i^{(2)}$ of minimal degree).

Anyway, our wish is to directly lift the modular separator polynomials that we obtain at the end of Algorithm 10, starting from the modular identity (4.4.1). A priori, fixing $P_i \mod p, \overline{P}_i \mod p$ which are not in $\mathfrak{a} \mod p$, there is only a finite number of monomials which can appear with non-zero coefficient in the reduced form of $P_i, \overline{P}_i$ with respect to $\mathfrak{a}$; the other information we have is that, on the contrary, $P_i\overline{P}_i \in \mathfrak{a}$, and so the leading monomial of $P_i\overline{P}_i$ with respect to a certain term order is a multiple of a monomial in the initial ideal of $\mathfrak{a}$.

Nevertheless, this information does not seem to be sufficient to obtain the lifting of $P_i\overline{P}_i \mod p$, as shown in the following example.

Example 4.4.1. *Consider the complete intersection ideal $\mathfrak{a}$ generated by*

$$F = 2\,X^2 + YX + 4\,X - Y - Z + 2,$$

$$G = ZYX - 4\,YX + 2\,Y^2 - 6\,ZX - ZY - Z^2 - 4\,Y - 10\,Z.$$

Applying Algorithm 10, we obtain that $\mathfrak{a}$ has only purely rational components, namely: $\mathfrak{q}_1$ and $\mathfrak{q}_2$ of degree and multiplicity 1 and $\mathfrak{q}_3$ of degree 4 and multiplicity 1.
More precisely, using $p = 127$, we obtain (in generic coordinates)

$$\begin{aligned} P_3^{(0)} \mod p = & ZYX + 11\,ZY^2 + 9\,Z^2X + 94\,Z^2Y + 31\,Z^3 + 69\,YX + 111\,Y^2 + \\ & + 83\,ZX + 90\,ZY + 117\,Z^2 + 56\,X + 46\,Y + 52\,Z + 6, \end{aligned}$$

$$\overline{P}_3^{(0)} \mod p := ZX + 55\,X + 66\,Z^2 + 93\,Z + 35\,ZY + 8 + 115\,Y.$$

We consider the linear system coming from the equality

$$(P_3^{(0)} + P_3^{(1)})(\overline{P}_3^{(0)} + p\overline{P}_3^{(1)}) \mod p^2 = (\eta^{(0)} + p\eta^{(1)})F + (\mu^{(0)} + p\mu^{(1)})G \mod p^2,$$

whose unknowns are the coefficients of $P_3^{(1)}$, $\overline{P}_3^{(1)}$, $\eta^{(1)}$, $\mu^{(1)}$. If we try to solve the linear system, we have not a unique solution for it. The same happens if we consider the linear system arising from the equalities

$$P_{3i}\overline{P}_{3i} \mod p^2 = \eta_i F + \mu_i G \mod p^2,$$

where $\{P_{3i} \mod p\}$ *is a set of generators of* $\mathfrak{q}_3$ *modulo* p*. Also in this case there are infinite solutions for the linear system.*

So, even if there is a finite number of choices for the monomials appearing with non-zero coefficient in the reduced form of $P_3 \mod p^2$ *with respect to* $\mathfrak{a}$ *(and the same for* $\overline{P}_3, \eta, \mu \mod p^2$*) and a finite number of choices for the coefficients of* $P_3^{(1)}$ *which are modulo* p*, we need to find other conditions, further then (4.4.2), which gives a unique solution to the problem.*

Example 4.4.1 is quite simple: the complete intersection considered has small degree, the primary components are all rational and prime. Despite this simple setting, the p-adic lifting of the separator polynomials is not easy at all.

Conclusions and future work

In this thesis, we have tried to solve in an explicit and constructive way the following problem:

> Given an *algebraic curve* in an affine space $\mathbb{C}^n$, defined by rational polynomials, find the equations defining its irreducible components.

We have studied the problem for $n = 2$ and $n = 3$.
For the case of a curve in $\mathbb{C}^2$, we have developed an absolute irreducibility test and an absolute factorization algorithm, using as main tools modular computations and p-adic approximations for algebraic numbers, with the LLL algorithm to recognize the approximated algebraic numbers. We tested the absolute factorization algorithm on many examples, using Maple; we could deal with high degree polynomials (up to 400); such high degrees were so far out of reach of all other absolute factorization algorithm; furthermore the computations in our tests are very fast on polynomials of middle degrees (about 100).

For what concerns curves in the affine space $\mathbb{C}^3$, we have drawn a parallel between the primary decomposition of an ideal and the absolute factorization of a polynomial, fixing it through definitions and properties. After that, we have investigated some bounds coming from algebraic geometry on the degree of a separator polynomial. We have then proved that modular computations generically preserve the Hilbert function of an ideal. This, with the classical technique of projection and quotient, gives us a modular algorithm that computes the Hilbert function of all the prime components of a complete intersection ideal in $\mathbb{Q}[X, Y, Z]$. We can use these results as a bound on the degree of a separator polynomial, helping a numerical algorithm in order to avoid extra and unnecessary computations. We have also adapted an existing algorithm for the computations of modular Groebner Basis; with the absolute factorization algorithm we have constructed, this gives another complete strategy to obtain the separator polynomials of the irreducible components.

In the next future, we would like to implement Algorithm 4. An efficient implementation will need good p-adic and X-adic Hensel liftings. We expect, in a near future, that the library Mathemagix [55] will provide optimized implementations of these routines. It will also be useful to have a "nice" presentation of the field extension, that is to consider a polynomial

$q(T)$ such that $\mathbb{L} \simeq Q[T]/q(T)$ and $q(T)$ has as small as possible coefficients. This will require the use of the PolRed Algorithm ([18]). Another point to improve is the parallel version of the algorithm, in order to be able to deal also with normal extensions of $\mathbb{Q}$.
We would also like to further investigate the techniques of p-adic approximation, in order to lift the modular bivariate factorization and recognize the algebraic coefficients directly, avoiding the specialization of variables and the subsequent X-adic Hensel lifting.

Concerning the decomposition of curves in the 3-dimensional space, we would like to improve it, namely to be able to lift the modular separators polynomials to separators in $\mathbb{Q}(\alpha)[X, Y, Z]$; this will be a generalization of the classical Hensel Lifting for modular factorizations. Another objective is the generalization of these techniques to curves which are not complete intersections. For this last problem, an obvious method is to compute the projection of the curves by using a generic change of coordinates, computing the resultants of all the couples of generators and considering the great common divisor of these resultants; however, we hope to do better, avoiding hard computations.

Furthermore, we would like to generalize the modular techniques of factorization to the decomposition of hypersurfaces in the n-dimensional affine space (that is, to absolute factorization of polynomials in n variables). The classical technique for multivariate absolute factorization is to specialize variables, use bivariate factorization (relying on Bertini's Theorem) and then perform X-adic Hensel liftings to reconstruct the multivariate factors. We expect that through modular techniques one can avoid the specialization of variables and the X-adic Hensel liftings, developing for the multivariate case too techniques of p-adic approximation and recognition of the coefficients.

Finally, once developed tools for curves in higher dimensions and for non-complete intersection curves in $\mathbb{C}^3$, we wish to investigate the decomposition of varieties of dimension m in the n-dimensional affine space, since the results about good reductions (see Section 4.2) hold for polynomial rings with n indeterminates and the technique of projection on linear hyperspaces stays true in higher dimension (see [73]).

Appendix

Appendix A

The LLL algorithm

Since the LLL algorithm is one of the main tools we used to reconstruct an algebraic number from its p-adic approximation, we recall here the main definitions and properties of integer lattices and present the LLL algorithm. For the omitted proofs, see [83], Chapter 8 and 9.

A.1 Lattices

Fix $d \geq 1$. Let $S \subseteq \mathbb{R}^d$ be a non-empty finite set. The lattice Λ generated by S is the set of integer linear combinations of the elements in S,

$$\Lambda = \Lambda(S) := \{m_1u_1 + m_2u_2 + \cdots + m_ku_k : k \geq 1, u_i \in S, m_i \in \mathbb{Z}\}.$$

The set S is called a *generating set* for the lattice Λ. If S has the minimum cardinality among generating sets for Λ, we call S a *basis* of Λ. The cardinality of a basis of Λ is the dimension, $\dim \Lambda$, of Λ.

Even for $d = 1$, the dimension of a lattice can be arbitrarily large or even infinite. But in our applications, it is sufficient to restrict Λ to the case where $u_1, \ldots, u_k$ are linearly independent as real vectors. In this case, $1 \leq k \leq d$. Looking at S as an ordered sequence $(u_1, \cdots, u_k)$ of vectors, we let

$$A = [u_1, \ldots, u_k] \in \mathbb{R}^{d\times k}$$

denote a $d \times k$ real matrix of rank k, and write $\Lambda(A)$ instead of $\Lambda(S)$. We say $\Lambda(A)$ is *full-dimensional* if and only if $k = d$.

A lattice Λ with only integer coordinates, $\Lambda \in \mathbb{Z}^d$, is called an *integer lattice*. The simplest example of a lattice is the unit integer lattice $\Lambda = \mathbb{Z}^d$. A basis for this lattice is the set $S = \{e_1, \ldots, e_d\}$ of elementary vectors in $\mathbb{R}^d$ (equivalently, the identity matrix $I = [e_1, \ldots, e_d]$ is a basis).

We examine the conditions for two bases A, B to generate the same lattice. If U is a $k \times k$ real non-singular matrix, we can transform a basis A to AU.

Definition A.1.1. *A square matrix $U \in \mathbb{C}^{k\times k}$ is* unimodular *if $\det U = 1$. A real, integer, etc, unimodular matrix is one whose entries are all real, all integer, etc.*

A unimodular matrix U represents a unimodular transformation of lattice bases, $A \mapsto AU$. Note that the inverse of a (real or integer, respectively) unimodular matrix is still (real or integer) unimodular.

Theorem A.1.2. *Let $A, B \in R^{d\times k}$ be two bases. Then $\Lambda(A) = \Lambda(B)$ if and only if there exists an integer unimodular matrix U such that $A = BU$.*

Definition A.1.3. *The determinant of a lattice Λ is given by*

$$\det \Lambda := \det \sqrt{A^T A}$$

where A is any basis with $\Lambda(A) = \Lambda$.

By definition, the determinant of a lattice is always positive. Using Theorem A.1.2, it is easy to show that $\det \Lambda$ is well-defined: if $A = BU$ for some unimodular matrix U (this demonstration does not depend on U being integer) then $\det A^T A = \det U^T B^T BU = \det(U^T) \det(B^T B) \det(U) = \det B^T B$. Geometrically, $\det \Lambda$ is the smallest volume of a parallelepiped formed by k independent vectors of Λ ($k = dim\Lambda$). For instance, the unit integer lattice has determinant 1. Another example is the lattice $\Lambda(u, v)$ where $u = (2, 1)^T$, $v = (3, 2)^T$. Actually this lattice is the whole space $\mathbb{Z}^2$. Note that $\det[u, v] = 1$.

It is easy to check that given any basis $A = [a_1, \ldots, a_n]$, the following transformations of A are unimodular transformations:

(i) multiplying a column of A by -1:

$$A = [a_1, \ldots, a_{i-1}, -a_i, a_{i+1}, \ldots, a_n];$$

(ii) adding a constant multiple c of one column to a different column:

$$A = [a_1, \ldots, a_j, \ldots, a_i + ca_j, \ldots, a_n];$$

(iii) permuting two columns of A:

$$A = [a_1, \ldots, a_{j-1}, a_i, a_{j+1}, \ldots, a_{i-1}, a_j, a_{i+1}, \ldots, a_n].$$

It is important that $i \neq j$ in (ii). We call these the *elementary column operations*.
If c in (ii) is an integer, then (i), (ii) and (iii) form the *elementary integer column operations*.
There is clearly an analogous set of elementary row operations. Together with the column ones, they are called the *elementary unimodular transformations*.
The unimodular matrices corresponding to the elementary transformations are called *elementary unimodular matrices*.

A fundamental result is that the group of unimodular matrices in $\mathbb{Z}^{n\times n}$ can be generated by the following three matrices (see [42],Theorem 3.1 page 382):

$$U_0 = \begin{bmatrix} -1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}, \quad U_1 = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & (-1)^{n-1} \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{bmatrix},$$

$$U_2 = \begin{bmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}.$$

It is easy to see that U_0, U_1, U_2 are each a product of elementary unimodular transformations. A matrix is unimodular if ad only if it is a product of the elementary unimodular transformations.

Let $|u|$ denote the (Euclidean) length of $u \in \mathbb{R}^d$: $|u| := \|u\|_2 = \sqrt{\sum_{i_1}^{d} u_i}$, in our general notation. When $d = 2$, this coincides with the absolute value of u as a complex number. The unit vector along direction u is $\hat{u} := u/|u|$. The scalar product of u, v is denoted by $\langle u, v\rangle$.

We have the basic inequality

$$|\langle u, v\rangle| \leq |u| \cdot |v|.$$

Remark that the zero vector $\mathbf{0}$ is always an element of a lattice. We define $u \in \Lambda$ to be a *shortest vector* in Λ if it has the shortest length among the non-zero vectors of Λ. More generally, we call a sequence $(u_1, u_2, \ldots, u_k), k \geq 1$, of vectors a *shortest k-sequence* of Λ if for each $i = 1, \ldots, k$, u_i is a shortest vector in the set $\Lambda(u_1, u_2, \ldots, u_{i-1})$. We call a vector a k-th shortest vector if it appears as the k-th entry in some shortest k-sequence.
We will not distinguish u from $-u$ when discussing shortest vectors. A fundamental computational problem in lattices is to compute another basis B for a given lattice $\Lambda(A)$ consisting of "short" vectors.

A.2 Gram-Schmidt Orthogonalization

Let $A = [a_1, \ldots, a_m] \in \mathbb{R}^{n \times m}$ be a lattice basis, $1 \leq m \leq n$. The matrix A is *orthogonal* if for all $1 \leq i < j \leq m$, $\langle a_i, a_j \rangle = 0$. There is a well-known strategy to convert A into an orthogonal basis $A^* = [a_1^*, \ldots, a_m^*]$:

Algorithm 12 Gram-Schmidt Procedure

Input: $A = [a_1, \ldots, a_m]$.

Output: $A^* = [a_1^*, \ldots, a_m^*]$ orthogonal matrix

1: $a_1^* := a_1$.
2: **for** for i from 2 to m **do**
3: **for** for j from 1 to $i - 1$ **do**
4: $\mu_{ij} := \frac{\langle a_i, a_j^* \rangle}{\langle a_j^*, a_j^* \rangle}$
5: **end for**
6: $a_i^* := a_i - \sum_{j=1}^{i-1} \mu_{ij} a_j^*$
7: **end for**
8: **return** $A^* = [a_1^*, \ldots, a_m^*]$

If we think of the case $m = 2, 3$, there is a clear way to visualize what happens when we substitute a_i with a_i^*: we are projecting a_i on the vectors space generated by the a_j^*, $j < i$, and then we take the vector a_i^* as the difference of a_i with this projection. The resulting matrix A^* is orthogonal (one can prove this by induction on m).

We call A^* is the *Gram-Schmidt version* of A. We say that two bases are Gram- Schmidt equivalent if they have a common Gram-Schmidt version.

Starting from the equation in Step 6 of Algorithm 12, we can define $\mu_{ii} := 1$ and so $a_i = \sum_{j=1}^{i} \mu_{ij} a_j^*$.

In matrix form, $A = A^* M^T$, where $A^* = [a_1, \ldots, a_m]$ and M^T is the transpose of a lower diagonal matrix

$$M = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ \mu_{21} & 1 & 0 & \cdots & 0 \\ \mu_{31} & \mu_{32} & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mu_{m1} & \mu_{m2} & \mu_{m3} & \cdots & 1 \end{bmatrix}.$$

The determinant of M is 1 and so the Gram-Schmidt version of A is a unimodular transformation of A. However, M need not be an integer matrix.

The number

$$\delta(A) := \frac{\|a_1\| \|a_2\| \cdots \|a_m\|}{\det(A^T A)}$$

is called the (orthogonality) *defect* of A. Note that $\delta(A) \geq 1$. Intuitively, it measures how far is A from its Gram-Schmidt version. We can then investigate the following problem: given a basis A, find another basis B with $\Lambda(A) = \Lambda(B)$ such that $\delta(B)$ is minimized.

A.3 The LLL algorithm

We now present the LLL algorithm, whose main aim is, given a lattice $\Lambda(A)$, find another basis of the lattice almost orthogonal. The basis found with LLL algorithm has another useful property: one vector of the new basis is almost as short as the shortest vector in $\Lambda(A)$.

A.3.1 Weakly reduced bases

A first step towards constructing bases with small defects, we introduce the concept of a weakly reduced basis.
Given a basis $B = [b_1, \ldots, b_m]$, we know that its Gram-Schmidt version $B^* = [b_1, \ldots, b_m]$ has no defect: $\delta(B^*) = 1$. Although B and B^* are related by a unimodular transformation M, unfortunately M is not necessarily integer.

So we would like to transform B via an integer unimodular matrix into some $\overline{B} = [\overline{b}_1, \ldots, \overline{b}_m]$ that is as close as possible to the Gram-Schmidt version. To make this precise, recall that for $i = 1, \ldots, m$,

$$b_i = \sum_{j=1}^{i} \mu_{ij} b_j^* \tag{A.3.1}$$

where $\mu_{ij} = \frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle}$, and $\mu_{ii} = 1$.

We say that B is *weakly reduced* if in the relation (A.3.1), the μ_{ij}'s satisfy the constraint

$$|\mu_{ij}| \leq \frac{1}{2}, \quad (1 \leq j < i \leq m).$$

Weakly reduced bases are as close to its Gram-Schmidt version as one can hope for, using only the elementary unimodular transformations but without permuting the columns. Let us consider how to construct such bases.

If B is not weakly reduced, there is a pair of indexes (i_0, j_0), $1 \leq j_0 < i_0 \leq m$, such that

$$|\mu_{i_0 j_0}| > \frac{1}{2}.$$

Pick (i_0, j_0) to be the lexicographically largest such pair: if $|\mu_{ij}| > 1/2$ then $(i_0, j_0) \geq_{Lex} (i, j)$, i.e., either $i_0 > i$ or $i_0 = i$, $j_0 \geq j$. Let

$$c_0 = \lfloor \mu_{i_0 j_0} \rceil$$

be the integer closest to $\mu_{i_0 j_0}$. Note that $c_0 \neq 0$. Consider the following unimodular transformation: we replace $B = [b_1, \ldots, b_{i_0}, \ldots, b_m]$ with $\overline{B} = [\overline{b}_1, \ldots, \overline{b}_{i_0}, \ldots, \overline{b}_m]$. where

$$\overline{b}_i = \begin{cases} b_i & \text{if } i \neq i_0 \\ b_{i_0} - c_0 b_{j_0} & \text{if } i = i_0. \end{cases}$$

We call the $B \to \overline{B}$ transformation a *weak reduction step*. We observe that B and $\overline{B}$ are Gram- Schmidt equivalent. So we may express $\overline{B}$ in terms of its Gram-Schmidt version (which is still $B^* = [b_1^*, \ldots, b_m^*]$) thus:

$$\overline{b}_i = \sum_{j=1}^{i} \overline{\mu}_{ij} b_j^*.$$

where it is easy to check that

$$\overline{\mu}_{ij} = \frac{\langle \overline{b}_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} = \begin{cases} \mu_{ij} & \text{if } i \neq i_0 \\ \mu_{ij} - c_0 \mu_{j_0 j} & \text{if } i = i_0 \end{cases}$$

In particular,

$$|\overline{\mu}_{i_0 j_0}| = |\mu_{i_0 j_0} - c_0| \leq \frac{1}{2}.$$

As usual, $\mu_{j_0 j} = 0$ if $j > j_0$. Hence, if (i, j) is any index such that $(i, j) >_{Lex} (i_0, j_0)$ then $\overline{\mu}_{ij} = \mu_{ij}$ so $|\overline{\mu}_{ij}| \leq \frac{1}{2}$. This immediately gives the following:

Lemma A.3.1 (Weak Reduction)**.** *Given any basis $B \in \mathbb{R}^{n \times m}$, we can obtain a weakly reduced basis $\overline{B}$ where $\Lambda(\overline{B}) = \Lambda(B)$ by applying at most $\binom{m}{2}$ weak reduction steps to B*

A.3.2 Reduced basis

Let us impose a restriction on weakly reduced bases B. A weakly reduced basis B is *reduced* if in addition it satisfies

$$\|b_i^*\|^2 \leq 2\|b_{i+1}\|^2$$

for $i = 1, \ldots, m-1$, where $B^* = [b_1^*, \ldots, b_m^*]$ is the Gram-Schmidt version of B. Actually reduced bases have bounded defect.

Lemma A.3.2. *If $B = [b_1, \ldots, b_m]$ is a reduced basis then its defect is bounded: $\delta(B) \leq 2^{\frac{1}{2}\binom{m}{2}}$.*

To measure how close a basis B is to being reduced, we introduce a real function $V(B)$ defined as follows:

$$V(B) := \prod_{i=1}^{m} V_i(B)$$

where

$$V_i(B) := \prod_{j=1}^{i} \|b_j^*\| = \sqrt{\det(B_i^T B_i)}$$

and B_i consists of the first i columns of B. Observe that $V_i(B)$ depends only on the Gram-Schmidt version of B_i. In particular, if B' is obtained by applying the weak reduction step to B, then $V(B') = V(B)$ since B' and B are Gram-Schmidt equivalent. Since $\|b_i\| \geq \|b_i^*\|$ for all i, we deduce that

$$V(B) = \prod_{i=1}^{n} \|b_i^*\|^{n-i+1} \leq \left(\max_i\{\|b_i\|\}\right)^{\binom{n}{2}}.$$

Now suppose $B = [b_1, \ldots, b_m]$ is not reduced by virtue of the inequality

$$\|b_i\|^2 > 2\|b_{i+1}\|^2$$

for some $i = 1, \ldots, m$. It is natural to perform the following reduction step which exchanges the i-th and $(i+1)$-st columns of B. Let the new basis be

$$C = [c_1, \ldots, c_m]$$

with $c_i = b_{i+1}$, $c_{i+1} = b_i$ and $c_j = b_j$ for $j \neq i$ or $i+1$. The choice of i for this reduction step is not unique. Nevertheless $V(B)$ is decreased.

Lemma A.3.3. *If C is obtained from B by a reduction step and B is weakly reduced then*

$$V(C) < \frac{\sqrt{3}}{2} V(B).$$

We describe the LLL algorithm in Algorithm 13.

Algorithm 13 LLL Algorithm

Input: $B \in \mathbb{Q}^{n \times m}$, a basis.

Output: A reduced basis $\overline{B}$ with $\Lambda(\overline{B}) = \Lambda(B)$.

1: $\overline{B}$:= weak-reduce(B).
2: **while** $\overline{B}$ is not reduced **do**
3: $\quad\overline{B}$:= reduce-step$(\overline{B})$.
4: $\quad\overline{B}$:= weak-reduce$(\overline{B})$.
5: **end while**
6: **return** $\overline{B}$.

We use *weak-reduce(B)* to denote a function call that returns a weakly reduced basis obtained by repeated application of the weak reduction step to B. Similarly, *reduce-step(B)* denotes a function that applies a single reduction step to a weakly-reduced B.

The algorithm stops after

$$\log_{\sqrt{3}/2} V(C) = O\left(n^2 \log\left(d\left(\max_i\{\|b_i\|\}\right)\right)\right) = O(n^2(s + \log n)),$$

reductions steps and gives a correct answer, with $\log \|b_i\| = O(s + \log n)$.

A.3.3 Short vectors

Let $B = [b_1, \ldots, b_m] \in \mathbb{R}^{n\times m}$ be a basis and let $\xi_1 \in \Lambda = \Lambda(B)$ denote the shortest lattice vector, $\xi_1 \neq 0$.

Using Minkowski's Convex Body Theorem, we can show that if Λ is a full-dimensional lattice, $\|\xi_1\|$ is bounded by $\sqrt{\frac{2n}{\pi}} \det(\Lambda)^{1/n}$. We do not even have an efficient algorithm to compute any lattice vector with length within this bound. But we can efficiently construct a vector ξ whose length is bounded by a slightly larger constant.

Moreover, there is a bound on $\|\xi\|$ involving the length of the shortest vector of $\Lambda(B)$: $\|\xi\|/\|\xi_1\| \leq 2^{(m-1)/2}$. Indeed, finding such a ξ is trivially reduced to the LLL-algorithm by showing that ξ can be chosen from a reduced base.

Lemma A.3.4. *Let $B^* = [b_1^*, \ldots, b_m^*]$ be the Gram-Schmidt version of B. Then the shortest vector ξ_1 satisfies*

$$\|\xi_1\| \geq \min_{i=1,\ldots,m} \|b_i^*\|.$$

We deduce from the above lemma:

Lemma A.3.5. *Let $B = [b_1, \ldots, b_m]$ be a reduced basis and ξ_1 be a shortest vector in $\Lambda(B)$.*

i) $\|b_1\| \leq 2^{(m-1)/2}\|\xi_1\|$,

ii) $\|b_1\| \leq 2^{(m-1)/4}(\det \Lambda(B))^{1/m}$.

Thus we can use the LLL-algorithm to construct a short vector ξ satisfying both

$$\|\xi\|/\|\xi_1\| \leq 2^{(m-1)/2} \quad \text{and} \quad \|\xi\| \leq 2^{(m-1)/4}(\det(B^T B))^{1/2m}.$$

A.4 Brief history of the LLL algorithm

The LLL algorithm is named by Arjen Lenstra, Hendrik Lenstra and László Lovász, the three authors of [53] where this algorithm first appeared in 1982.

This paper describes an algorithm for rational factorization of a univariate polynomial which can be performed in polynomial time. The idea is to find a p- adic factor of the polynomial (using modular computations and Hensel lifting) and establish a connection between this p-adic approximation and the true factor by means of an integer lattice.

The authors are interested in finding a short vector of an integer lattice, that is why they present a *lattice reduction algorithm*, which is the (nowadays) well-known LLL algorithm.

In the following years this algorithm found many other applications, most of them in number theory and cryptography: we may cite as examples the application to the knapsack problem ([43]), the construction of minimal polynomial from a numeric approximation of an algebraic number ([47]), and in general to all problems concerning the search for integer relations between vectors.

Nevertheless the LLL algorithm has a bad complexity from the theoretical point of view. A very recent paper, [61], modifies the LLL algorithm improving the complexity bound.

Also other algorithms to find integer relations between numeric approximations were developed, for instance the $PSLQ$ algorithm (see [26]), which also works on a integer lattice, but is not a lattice reduction algorithm; it is based on a partial sum of squares scheme implemented using QR decomposition.

Appendix B

p-adic numbers

If we start considering the field of rational numbers $\mathbb{Q}$, we can get its completion according to the "usual" norm (that is, the usual way to measure the distance between to numbers), obtaining the field $\mathbb{R}$. In a few words, we are adding to $\mathbb{Q}$ all the points of convergence of Cauchy sequence with rational elements.

What happens if we change the usual way to measure distances?

B.1 p-adic absolute value

We start considering a field $\mathbb{K}$ and define what is an absolute value.

Definition B.1.1. *An* absolute value *on* $\mathbb{K}$ *is a function*

$$|\cdot| : \mathbb{K} \to \mathbb{R}_+$$

that satisfies the following conditions:

1. $|x| = 0$ *if and only if* $x = 0$*;*
2. $|xy| = |x| \cdot |y|$ *for all* $x, y \in \mathbb{K}$*;*
3. $|x + y| \leq |x| + |y|$ *for all* $x, y \in \mathbb{K}$*.*

The absolute values is non-archimedean *if it satisfies the additional condition*

4. $|x + y| \leq \max\{|x|, |y|\}$ *for all* $x, y \in \mathbb{K}$*;*

otherwise, we will say that the absolute value is archimedean*.*

In what follows we are interested in two different kinds of absolute values defined on $\mathbb{Q}$.

Example B.1.2. *Consider the absolute value*

$$|x|_\infty = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$$

This absolute value is well-known, we are using the unusual notation with "∞" to avoid confusion with the other absolute value we are interested in. This absolute value is archimedean.

Example B.1.3. *Fix a prime integer $p \in \mathbb{Z}$ and consider $a \in \mathbb{Z}$.*

Let l be the highest integer such that p^l divides a. Then the p-adic absolute value *on integers is*

$$|a|_p = p^{-l}$$

In other words, the p-adic absolute value of a number measures how divisible it is by p: the smallest is the absolute value, the highest is the divisibility.

We can naturally extend this absolute value on the integers to an absolute values on the rational:
for every $\frac{a}{b} \in \mathbb{Q}$ such that $\gcd(a, b) = 1$, there is a unique way to write it as

$$\frac{a}{b} = \frac{r}{s}p^l \quad \text{with } \gcd(r, s) = 1, p \nmid r, s.$$

We can then define the p-adic absolute values of $\frac{a}{b}$:

$$\left|\frac{a}{b}\right|_p = p^{-l}.$$

$|\cdot|_p$ is a non-archimedean absolute value.

In what follows, we will keep on using the notation $|\cdot|_\infty$ for the "usual" absolute value, $|\cdot|_p$ for the p-adic absolute value and simply $|\cdot|$ if we want to refer to *an* absolute value on a field $\mathbb{K}$.

Definition B.1.4. *Let $\mathbb{K}$ be a field and $|\cdot|$ an absolute value on $\mathbb{K}$. We define the* distance *$d(x, y)$ between two elements $x, y \in \mathbb{K}$ as*

$$d(x, y) := |x - y|.$$

The function $d(x, y)$ is called the metric *induced by the absolute value. A metric $d(x, y)$ has the following properties:*

1. *for any $x, y \in \mathbb{K}$, $d(x, y) \geq 0$ and $d(x, y) = 0$ if and only if $x = y$;*
2. *for any $x, y \in \mathbb{K}$, $d(x, y) = d(y, x)$;*
3. *for any $x, y, z \in \mathbb{K}$, $d(x, z) \leq d(x, y) + d(y, z)$.*

Lemma B.1.5. *Let $|\cdot|$ be an absolute value on a field $\mathbb{K}$ an define a metric $d(x,y) = |x-y|$. Then $|\cdot|$ is non-archimedean of and only if for any $x, y, z \in \mathbb{K}$ we have*

$$d(x,z) \leq \max\{d(x,y), d(y,z)\}. \tag{B.1.1}$$

The inequality (B.1.1) is called *ultrametric inequality* and a metric for which is true is called *ultrametric*.

If we consider an ultrametric $d(\cdot,\cdot)$ on $\mathbb{K}$ we have some nice and curious consequences on geometry and topology: for instance all the "triangles" are isosceles (see [34], section3.2).

If we define an *open ball* of center a radius r as

$$B(a,r) = \{x \in \mathbb{K} | d(x,a) < r\} = \{x \in \mathbb{K} | |x-a| < r\}$$

then we have that with the topology inducted by the metric $d(x,y)$, balls are at the same time open and closed and every point contained in a ball is its center (see [34], section 2.3).

B.2 Completion

Definition B.2.1. *Consider an absolute value $|\cdot|$ on a field $\mathbb{K}$.*

1. *A sequence of elements $x_n \in \mathbb{K}$ is a* Cauchy sequence *if for every $\epsilon > 0$ one can find a bound M such that we have $|x_n - x_m| < \epsilon$ whenever $n, m \geq M$;*

2. *$\mathbb{K}$ is* complete *with respect to $|\cdot|$ if every Cauchy sequence of elements of $\mathbb{K}$ has a limit in $\mathbb{K}$;*

3. *a subset $S \subseteq \mathbb{K}$ is* dense *in $\mathbb{K}$ if every open ball around every element of $\mathbb{K}$ contains an element of S.*

The field of rational numbers $\mathbb{Q}$ is not complete nor with respect to the absolute value $|\cdot|_\infty$ or $|\cdot|_p$. The field of real numbers $\mathbb{R}$ is the *completion* of $\mathbb{Q}$ with respect to $|\cdot|_\infty$.

How about the completion with respect to $|\cdot|_p$? We briefly recall the construction of the completion of $\mathbb{Q}_p$, for details see [34], section 3.2.

- $\mathcal{C} = \mathcal{C}_p(\mathbb{Q}) := \{(x_n) | (x_n)$ is a Cauchy sequence with respect to $\mathbb{Q}\}$;
- we define on $\mathcal{C}$ a sum and a product such that $\mathcal{C}$ is a commutative ring with identity;
- we can include $\mathbb{Q}$ in $\mathcal{C}$;
- $\mathcal{N} := \{(x_n) \in \mathcal{C} | \lim_{n\to\infty} |x_n|_p = 0\}$ is a maximal ideal in $\mathcal{C}$;

- finally, we define the *field of p-adic numbers* $\mathbb{Q}_p$ to be the quotient of the ring $\mathcal{C}$ by its maximal ideal $\mathcal{N}$. Through the inclusion in $\mathcal{C}$, $\mathbb{Q}$ can be included in $\mathbb{Q}_p$.

We can extend the absolute value $|\cdot|_p$ to $\mathbb{Q}_p$.

Definition B.2.2. *If $\lambda \in \mathbb{Q}_p$ is an element of $\mathbb{Q}_p$ and (x_n) is any Cauchy sequence representing λ, we define*

$$|\lambda|_p = \lim_{n\to\infty} |x_n|_p.$$

The definition is compatible with the classes of equivalence of $\mathbb{Q}_p$ (see [34], section 3.2).

Remark that the image of $\mathbb{Q}$ under $|\cdot|_p$ is the same as the image of $\mathbb{Q}_p$ under $|\cdot|_p$: this means that for every $\lambda \in \mathbb{Q}_p$, $\lambda \neq 0$, there exist $n \in \mathbb{Z}$ such that $|\lambda|_p = p^{-n}$.

Proposition B.2.3.

1. *The image of $\mathbb{Q}$ under the inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ is a dense subset of $\mathbb{Q}_p$.*
2. *$\mathbb{Q}_p$ is complete with respect to the absolute value $|\cdot|_p$.*

B.3 Algebraic extensions

As we stated, the fields $\mathbb{R}$ and $\mathbb{Q}_p$ solve the problem of convergence of Cauchy sequences in $\mathbb{Q}$, according to the way we are measuring distances.

There is one problem left: in the same way as $\mathbb{R}$ is not algebraically closed, $\mathbb{Q}_p$ is neither. For instance, if we are considering a prime p such that 2 is not a square in $\mathbb{Q}_p$, then we can consider the extension $\mathbb{K} = \mathbb{Q}_p(\sqrt{2})$.

In general, let $\mathbb{K}$ be a field containing $\mathbb{Q}_p$. This means that $\mathbb{K}$ is a vector space on $\mathbb{Q}_p$ and it is a finite extension if its dimension as vector space on $\mathbb{Q}_p$ is finite. As usual, $[\mathbb{K} : \mathbb{Q}_p] = \dim_{\mathbb{Q}_p} \mathbb{K}$ is the degree of extension of $\mathbb{K}$ on $\mathbb{Q}_p$.

We would like to define an absolute value $|\cdot|$ on $\mathbb{K}$, obviously satisfying properties 1., 2., 3. of definition B.1.1 and the extra one:

4. $|\lambda| = |\lambda|_p$ whenever $\lambda \in \mathbb{Q}_p$.

Assume that $\mathbb{K}$ is a normal extension on $\mathbb{Q}_p$. We then have a finite set of automorphism σ of $\mathbb{K}$ fixing $\mathbb{Q}_p$ (and the cardinality of this finite set is exactly $[\mathbb{K} : \mathbb{Q}_p] = n$).

Then, we can define the *norm* of $\alpha \in \mathbb{K}$ as

$$N_{\mathbb{K}/\mathbb{Q}_p}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

Observe that $N_{\mathbb{K}/\mathbb{Q}_p}(\alpha) \in \mathbb{Q}_p$.

Theorem B.3.1. *Let $\mathbb{K}$ a finite extension of $\mathbb{Q}_p$ of degree n. The function $|\cdot| : \mathbb{K} \to \mathbb{R}_+$ defined by*

$$|x| = \sqrt[n]{|N_{\mathbb{K}/\mathbb{Q}_p}(x)|_p}$$

is a non-archimedean absolute value which extends the p-adic absolute value on $\mathbb{Q}_p$.

This is the unique p-adic absolute value on $\mathbb{K}$ extending the p-adic absolute value on $\mathbb{Q}_p$ and $\mathbb{K}$ is complete with respect to this.

Example B.3.2. *Consider $\mathbb{Q}_7$ and α root of $q(T) = T^2 - 2$. The automorphisms of $\mathbb{K} = \mathbb{Q}_7(\alpha)$ fixing $\mathbb{Q}_7$ are σ_1, the identity, and $\sigma_2(\alpha) = -\alpha$. Then the p-adic absolute value on $\mathbb{K}$ is*

$$N_{\mathbb{K}/\mathbb{Q}_7}(a) = \sqrt[2]{|\sigma_1(a)\sigma_2(a)|_7}.$$

For instance, the p-adic absolute value of $1 + 5\alpha$ in $\mathbb{K}$ is

$$N_{\mathbb{K}/\mathbb{Q}_7}(1 + 5\alpha) = \sqrt[2]{|(1 + 5\alpha)(1 - 5\alpha)|_7} = \frac{1}{7}.$$

Obviously, if we compute the p-adic absolute values in $\mathbb{K}$ of $a \in \mathbb{Q}_7$, this is just its usual p-adic absolute value; for instance, consider $a = 4$:

$$N_{\mathbb{K}/\mathbb{Q}_7}(4) = \sqrt[2]{|4^2|_7} = 1.$$

B.4 p-adic expansions

Just like when we work with real numbers, we can approximate rational and algebraic numbers through their p-adic expansions.

We will show with some examples how this expansions can be computed to a certain level of accuracy and in the next section we will show the theoretical foundations of these techniques.

Example B.4.1. *Consider the integer 27 and compute its 5-adic expansion*

- *the first digit is the remainder of the division $27/5$, so the first digit is $\alpha_0 = 3$.*
- *the second digit is $\alpha_1 \in \{0, \ldots, 4\}$ such that $|27 - 3 \cdot 5^0 - \alpha_1 \cdot 5^1|_5$ is maximal: in this case $\alpha_1 = 0$.*
- *the third digit is $\alpha_2 \in \{0, \ldots, 4\}$ such that $|27 - 3 \cdot 5^0 - 0 \cdot 5^1 - \alpha_2 \cdot 5^2|_5$ is maximal: in this case $\alpha_2 = 2$.*

So

$$27 = 3 \cdot 5^0 + 0 \cdot 5^1 + 2 \cdot 5^2.$$

We will also use the notation $27 = 203_5$.

Example B.4.2. *We now compute using the same technique of example B.4.1 the* 13*-adic expansion of* $24/17$*.*

- *the first digit is* $\alpha_0 \in \{0, \dots, 12\}$ *such that* $|24/17 - \alpha_0|_{13}$ *is maximal:* $\alpha_0 = 6$*.*
- *the second digit is* $\alpha_1 \in \{0, \dots, 12\}$ *such that* $|24/17 - 6 \cdot 13^0 - \alpha_1 \cdot 13^1|_{13}$ *is maximal:* $\alpha_1 = 5$*.*
- *the third digit is* $\alpha_2 \in \{0, \dots, 12\}$ *such that* $|24/17 - 6 \cdot 13^0 - 5 \cdot 13^1 - \alpha_2 \cdot 13^2|_{13}$ *is maximal:* $\alpha_2 = 7$*.*

Keeping on computing, we obtain

$$\frac{24}{17} = \dots 78547856_{13}.$$

It may be interesting to see that the behaviour of the usual decimal expansion of $a \in \mathbb{Q}$ may not be the same of the behaviour of the p-adic expansion of the same a: that is, if from a certain digit the decimal expansion of a is made up of 0's (the decimal expansion is *finite*), it may not happen for the p-adic expansion.

Example B.4.3. *We now compute the* 11*-adic expansion of* $1/5$*.*

- *the first digit is* $\alpha_0 \in \{0, \dots, 10\}$ *such that* $|1/5 - \alpha_0|_{11}$ *is maximal:* $\alpha_0 = 9$*.*
- *the second digit is* $\alpha_1 \in \{0, \dots, 10\}$ *such that* $|1/5 - 9 \cdot 11^0 - \alpha_1 \cdot 11^1|_{11}$ *is maximal:* $\alpha_1 = 8$*.*
- *the third digit is* $\alpha_2 \in \{0, \dots, 10\}$ *such that* $|1/5 - 9 \cdot 11^0 - 8 \cdot 11^1 - \alpha_2 \cdot 11^2|_{11}$ *is maximal:* $\alpha_2 = 8$*.*

Keeping on computing, we obtain

$$\frac{1}{5} = \dots 888889_{11}.$$

Remark that $1/5$ *has a finite expansion using decimal digits:* $1/5 = 0.20000000\dots$*; while using* 11*-adic expansion, there are infinite non-zero p-adic digits.*

Also the inverse may happen: an infinite decimal expansion may correspond to a finite p-adic expansion

Example B.4.4. *We now compute the* 7*-adic expansion of* $44/49$*. If we try, as in the previous examples, to find the digits such that* $|44/49 - \sum_{i=0}^{m} \alpha_i \cdot 7^i|_7$ *is maximal, for* m *starting from 0, we will obtain* $\alpha_i = 0$ *for all* i*.*

We have to try with negative *powers of 7, so we look for digits wit a negative index.*

- *the first digit is* $\alpha_{-1} \in \{0, \ldots, 6\}$ *such that* $|1/5 - \alpha_{-1} \cdot 7^{-1}|_7$ *is maximal:* $\alpha_{-1} = 6$.
- *the second digit is* $\alpha_{-2} \in \{0, \ldots, 10\}$ *such that* $|1/5 - 6 \cdot \cdot 7^{-1} - \alpha_{-2} \cdot 7^{-2}|_7$ *is maximal:* $\alpha_{-2} = 2$.

There are no more non-zero digits to compute, since

$$\frac{44}{49} = 6 \cdot 7^{-1} + 2 \cdot 7^{-2}.$$

So, the 7*-adic expansion of* $44/49$ *is*

$$\frac{44}{49} = 0.62_7$$

The last example is interesting for 2 different reasons.

First of all, we have an example of a rational number with infinite decimal expansion

$$\frac{44}{49} = 0.\overline{897959183673469387755102040816326530612244}$$

with a finite p-adic expansion.

Furthermore, the other examples were concerning rational numbers whose image in $\mathbb{Q}_p$ is actually a p-adic integer (it is $\in \mathbb{Z}_p$). Without using complicated details, we can see this just observing the p-adic expansions: if the digits are on the left of the point (that is: we are using only non negative powers of p to write the expansion), then the numbers are p-adic integers. If there are non-zero digits on the right of the point, then the number is not a p-adic integer (that is, we are using negative powers of p in the expansion).

Example B.4.5. *The* 5*-adic expansion of* $58/75$ *is*

$$\frac{58}{75} = \ldots 313131313132.21_5$$

We are also able to compute p-adic expansion also for algebraic numbers, if p is "well-chosen". The idea is the same as in Lemma 1.4.9: we choose α algebraic number on $\mathbb{Q}$ and if we have a prime p such that the minimal polynomial of α factors modulo p, with a linear factor, then we can have a p-adic expansion of α.

Example B.4.6. *Consider* α*, sum of a square root of* 2 *and a primitive cube root of the unity. The minimal polynomial of* α *is* $q(T) = T^4 - 2T^3 - T^2 + 2T + 7$*. We choose* $p = 31$*, since* $q(T)$ *factors modulo* p*: it is a product of linear factors.*

If we look for p*-adic approximation of the roots of* $q(T)$*, then we look for* p*-adic numbers* γ *such that the value* $q(\gamma)$ *is minimal with respect to the* p*-adic absolute value. We then proceed just like we did for rational numbers:*

- *we look for* $\alpha_0 \in \{0, \ldots, 30\}$*, first digit of the* p*-adic expansion, such that* $|q(\alpha_0)|_{31}$ *is minimal; we find that four values have the same minimal absolute value:* $\alpha_0 \in \{3, 14, 18, 29\}$*;*

- *we look for* α_1*, the second digit, such that* $|q(\alpha_0 + \alpha_1 \cdot 31)|_{31}$ *is minimal; we find out the following couples of* (α_0, α_1) *minimizing the absolute value:* $(3, 13)$*,* $(14, 10)$*,* $(18, 20)$ *and* $(29, 17)$*.*

Going on with the same technique, we find the p*-adic approximations of the roots of the polynomial* $q(T) = T^4 - 2T^3 - T^2 + 2T + 7$*:*

$$\ldots(4)(9)(13)(3)_{31},\ \ldots(21)(27)(10)(14)_{31},\ \ldots(9)(3)(20)(18)_{31},\ \ldots(26)(21)(17)(29)_{31}.$$

It is clear that the first digit α_0 *is one of the roots of* $q(T) \mod p$*.*

B.5 Hensel's lifting

One of the most interesting tools linking polynomials in the field of p-adic numbers and rational polynomials in Hensel's Lemma. All the examples of the previous section are actually based on it. We first enunciate its original form, which is the theoretical tool hidden in the examples of the previous sections, and then concentrate on a second form which is in connection with rational polynomial factorization.

Theorem B.5.1 (Hensel's Lemma)**.** *Let* $F(X) = \sum_{i=1}^{n} a_i X^i$ *be a polynomial with coefficients in* $\mathbb{Z}_p$*. Suppose there exists a* p*-adic integer* α_1 *such that*

$$F(\alpha_1) \equiv 0 \mod p\mathbb{Z}_p \quad \textit{and} \quad F'(\alpha_1) \not\equiv 0 \mod p\mathbb{Z}_p$$

where $F'(X)$ *is the derivative of* $F(X)$*. Then there exists a* p*-adic integer* α *such that* $\alpha \equiv \alpha_1 \mod p\mathbb{Z}_p$ *and* $\mathbb{F}(\alpha) = 0$*.*

We now show another version of Hensel's Lemma, adapted to the case of polynomials in $\mathbb{Z}[X]$. $\mathbb{Z}_p$ is the ring of p-adic integers.

Theorem B.5.2 (Hensel's Lemma second form)**.** *Let* p *be a prime in* $\mathbb{Z}$ *and let* $a(X) \in \mathbb{Z}[X]$ *be a given polynomial. Let* $u^{(1)}(X), w^{(1)}(X) \in \mathbb{Z}/p\mathbb{Z}[X]$ *be two relatively prime polynomials over the field* $\mathbb{Z}/p\mathbb{Z}$ *such that*

$$a(X) = u^{(1)}(X)w^{(1)}(X) \mod p.$$

Then there exist polynomials $u^{(\lambda)}(X), w^{(\lambda)}(X) \in \mathbb{Z}_p[X]$*such that*

$$a(X) = u^{(\lambda)}(X)w^{(\lambda)}(X) \textit{ in } \mathbb{Z}_p[X]$$

and

$$u^{(\lambda)}(X) \equiv u^{(1)}(X) \mod p, \quad w^{(\lambda)}(X) \equiv w^{(1)}(X) \mod p.$$

The proof of this version of Hensel's Lemma (see [81], Theorem 15.11 and 15.12) is constructive. We just show the construction of $u^{(2)}(X)$ and $w^{(2)}(X)$; the same construction applies inductively.

Since $u^{(1)}(X), w^{(1)}(X) \in \mathbb{Z}/p\mathbb{Z}[X]$ are relatively prime, there are $s, t \in \mathbb{Z}[X]$ such that $su^{(1)} + tw^{(1)} \equiv 1 \mod p$. We now compute

$$e = a - u^{(1)}w^{(1)}, \quad \hat{u} = u^{(1)} + te, \quad \hat{w} = w^{(1)} + se,$$

and find

$$\begin{aligned} &a - \hat{u}\hat{v} = f - u^{(1)}w^{(1)} - u^{(1)}se - w^{(1)}te - ste^2 = \\ &= f - u^{(1)}w^{(1)} - (su^{(1)} + tw^{(1)})e - ste^2 = (1 - su^{(1)} - tw^{(1)})e - ste^2 \equiv 0 \mod p^2, \end{aligned}$$

since $e \equiv 0 \mod p$ and $1 - su^{(1)} - tw^{(1)} \equiv 0 \mod p$. Hence $a \equiv \hat{u}\hat{w} \mod p^2$, so that $\hat{u}\hat{w}$ is a factorization of a modulo p^2. Proceeding inductively (and simultaneously lifting the congruence $su^{(\lambda)} + tu^{(\lambda)} \equiv 1 \mod p^\lambda$), we can lift the factorization modulo arbitrary powers of p.

Algorithm 14 Hensel Step

Input: $a \in \mathbb{Z}[X]$, p prime integer, $u, w \in \mathbb{Z}[X]$ relatively prime, w monic such that $a = uw \mod p$, $\deg a = \deg u + \deg w$
$s, t \in \mathbb{Z}[X]$ such that $su + tw \equiv 1 \mod p$, $\deg s < \deg w$, $\deg r < \deg u$,

Output: polynomials $u^*, w^*, s^*, t^* \in \mathbb{Z}[X]$ such that

$$a(X) = u^*(X)w^*(X) \mod p^2 \qquad s^*u^* + t^*w^* \equiv 1 \mod p^2$$

with w^* monic, $u^* \equiv u \mod p$,$w^* \equiv w \mod p$, $s^* \equiv s \mod p$, $t^* \equiv t \mod p$
$\deg u^* = \deg u$, $\deg w^* = \deg w$, $\deg s^* < \deg w^*$, $\deg t^* < \deg u^*$.

1: $b := a - uw \mod p^2$
2: Compute the Euclidean division: $sb = qw + r \mod p^2$ with $\deg r < \deg h$
3: $u^* := u + tb + qu \mod p^2$
4: $w^* := w + r \mod p^2$
5: $c := su^* + tw^* - 1 \mod p^2$
6: Compute the Euclidean division: $sc = dw^* + e$ with $\deg e < \deg w^*$
7: $s^* = s - e \mod p^2$
8: $t^* = t - tc - du^* \mod p^2$
9: **return** u^*, w^*, s^*, t^*.

B.6 Farey fractions

It is natural to ask: when we reduce a rational number a/b modulo a prime p, obtaining c, can we recover a/b from the knowledge of c and p? Or better, when we approximate p-adically a rational number, how can we recover it?

Definition B.6.1. *Let N be a positive integer. The reduced order-N Farey fractions are*

$$F_N = \left\{ \frac{a}{b} | \gcd(a,b) = 1, 0 \leq a \leq N, 0 < |b| \leq N \right\}.$$

We now fix a prime integer p and N, the biggest positive integer such that

$$N \leq \sqrt{\frac{p-1}{2}}. \tag{B.6.1}$$

There is a natural way to map the Farey fractions of order N into the finite field $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$:

$$\begin{aligned} \varphi_p : F_N &\to \mathbb{F}_p \\ \frac{a}{b} &\mapsto (a \mod p)(b^{-1} \mod p). \end{aligned}$$

Thanks to (B.6.1), φ_p is one-to-one mapping between F_N and $\mathbb{F}_p$, and so it is possible to construct the inverse mapping. Actually, instead of considering a prime p, we can consider $m = p^r$ and choose the biggest integer N such that

$$N \leq \sqrt{(p^r - 1)/2}. \tag{B.6.2}$$

It is possible to define φ_m and to look for the inverse mapping. For every $c \in \mathbb{F}_m$, it is possible to compute $a/b \in F_N$ such that $\varphi_m(a/b) = c$.

Algorithm 15 is fully described in [48], where it is proved that the algorithm stops and that the couple (a_i, b_i) such that $a_i/b_i \in F_N$ is unique.

Example B.6.2. *Consider the Farey fractions F_{17} and consider $p = 625$.*
We consider $\varphi_p(10/13) = 145$ and we apply the algorithm to recover $10/13$ starting with the seed matrix

$$\begin{bmatrix} 625 & 0 \\ 145 & 1 \end{bmatrix}.$$

The iterations are summarized in the following table

i	q_i	a_i	b_i
-2	*-*	*625*	*0*
-1	*-*	*145*	*1*
0	*4*	*45*	*-4*
1	*3*	*10*	*13*
2	*4*	*5*	*-56*
3	*2*	*0*	*125*

Algorithm 15 Recognition of Farey fractions

Input: p prime integer, $m = p^r$ with $r \geq 1$, N the biggest positive integer such that $N \leq \sqrt{(p^r - 1)/2}$, $c \in \mathbb{F}_m$.

Output: $a/b \in F_N$ such that $\varphi_m(a/b) = c$.

1: Consider the *seed matrix*
$$\begin{bmatrix} a_{-2} & a_{-1} \\ b_{-2} & b_{-1} \end{bmatrix} = \begin{bmatrix} p & 0 \\ c & 1 \end{bmatrix}.$$
2: $i := 1$
3: **while** $a_{i-1} \neq 0$ **do**
4: compute q_i as the quotient the Euclidean division of a_{i-2} with respect to a_{i-1} and a_i as the non-negative remainder:
$$a_i = a_{i-2} - q_i a_{i-1}.$$
5: $b_i := b_{i-2} - q_i b_{i-1}$
6: $i := i + 1$
7: **end while**
8: **return** the only couple (a_i, b_i) such that $0 \leq a_i \leq N$, $0 < |b_i| \leq N$

The algorithm stops at $i = 3$, since $a_3 = 0$. The only couple (a_i, b_i) such that $a_i/b_i \in F_{17}$ is $(a_1, b_1) = (10, 13)$.

Obviously, Algorithm 15 can be used to recover from a p-adic expansion of a rational number, once that we have a bound on the size of the numerator and denominator of the rational we are looking for.

Example B.6.3. *Consider $p = 5$, $m = 625$, we consider the first 4 digits of the p-adic expansion of a rational number, $c = 1314_5$; assume also that the size of the numerator and of the denominator of the fraction we are looking for is bounded by $N = 17$.*
We can apply Algorithm 15 (N satisfies condition (B.6.2)), we obtain the following values in the iterations

i	q_i	a_i	b_i
-2	*-*	*625*	*0*
-1	*-*	*209*	*1*
0	*2*	*207*	*-2*
1	*1*	*2*	*3*
2	*103*	*1*	*-311*
3	*2*	*0*	*625*

The couple (a_1, b_1) gives a fraction contained in F_N, $\frac{2}{3}$.

So if we have the first r digits of a p-adic expansion of a rational number and we know that the size of its numerator and denominator is bounded by N satisfying (B.6.2) for p^r, then we can reconstruct the rational number through Algorithm 15.

Bibliography

[1] Elizabeth A. Arnold. Modular algorithms for computing Gröbner bases. *J. Symb. Comput.*, 35(4):403–419, 2003.

[2] Michael F. Atiyah and Ian G. Macdonald. *Introduction to commutative algebra.* Reading, Mass.-Menlo Park, Calif.- London-Don Mills , Ont.: Addison- Wesley Publishing Company , 1969.

[3] Dave Bayer and David Mumford. What can be computed in algebraic geometry? Eisenbud, David (ed.) et al., Computational algebraic geometry and commutative algebra. Proceedings of a conference held at Cortona, Italy, June 17-21, 1991., 1993.

[4] Cristina Bertone. The Euler characteristic as a polynomial in the Chern classes. *Int. J. Algebra*, 2(13-16):757–769, 2008.

[5] Cristina Bertone, Guillaume Chèze, and André Galligo. Modular Las Vegas Algorithms for Polynomial Absolute Factorization. Available on http://hal.inria.fr/inria-00436063/fr/ , submitted, 2009.

[6] Cristina Bertone and Margherita Roggero. Positivity of Chern classes for reflexive sheaves on P^N. *Geom. Dedicata*, 142:121–138, 2009.

[7] Cristina Bertone and Margherita Roggero. Splitting type, global sections and Chern classes for vector bundles on P^N. *J. Korean Math. Soc.*, to appear.

[8] Alin Bostan, Grégoire Lecerf, Bruno Salvy, Éric Schost, and B. Wiebelt. Complexity issues in bivariate polynomial factorization. Gutierrez, Jaime (ed.), ISSAC 2004. Proceedings of the 2004 international symposium on symbolic and algebraic computation, Santander, Spain, July 4–7, 2004. New York, NY: ACM Press. 42-49, 2004.

[9] Richard L. Burden and J.Douglas Faires. *Numerical analysis. 5th ed.* Boston, MA: PWS Publishing Company. London: ITP International Thomson Publishing, xiv, 768 p., 1993.

[10] Guido Castelnuovo. Sui multipli di una serie lineare di gruppi di punti appartenente ad una curva algebrica. 1893.

[11] Marc Chardin. Cohomology of projective schemes: From annihilators to vanishing. *J. Algebra*, 274(1):68–79, 2004.

[12] Marc Chardin and Patrice Philippon. Regularity and interpolation. (Régularité et interpolation.). *J. Algebr. Geom.*, 8(3):471–481, 1999.

[13] Marc Chardin and Bernd Ulrich. Liaison and Castelnuovo-Mumford regularity. *Am. J. Math.*, 124(6):1103–1124, 2002.

[14] Guillaume Chèze. *Des méthodes symboliques-numériques et exactes pour la factorisation absolue des polynômes en deux variables*. PhD thesis, Université de Nice, France, 2004.

[15] Guillaume Chèze and André Galligo. Four lectures on polynomial absolute factorization. Dickenstein, Alicia (ed.) et al., Solving polynomial equations. Foundations, algorithms, and applications. Berlin: Springer. Algorithms and Computation in Mathematics 14, 339-392, 393–418, 2005.

[16] Guillaume Chèze and Grégoire Lecerf. Lifting and recombination techniques for absolute factorization. *J. Complexity*, 23(3):380–420, 2007.

[17] Francesca Cioffi, Maria Grazia Marinari, and Luciana Ramella. Regularity bounds by minimal generators and Hilbert function. *Collect. Math.*, 60(1):89–100, 2009.

[18] Henri Cohen and Francisco Diaz y Diaz. A polynomial reduction algorithm. *Sémin. Théor. Nombres Bordx., Sér. II*, (1):351–360, 1991.

[19] David Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra. 2nd ed.* Undergraduate Texts in Mathematics. New York, NY: Springer. xiii, 536 p., 1996.

[20] Pierre Dèbes and Yann Walkowiak. Bounds for Hilbert's irreducibility theorem. *Pure Appl. Math. Q.*, 4(4):1059–1083, 2008.

[21] Wolfram Decker, Gert-Martin Greuel, and Gerhard Pfister. Primary decomposition: algorithms and comparisons. In *Algorithmic algebra and number theory (Heidelberg, 1997)*, pages 187–220. Springer, Berlin, 1999.

[22] Wolfram Decker and Christoph Lossen. *Computing in algebraic geometry. A quick start using SINGULAR.* Algorithms and Computation in Mathematics 16. Berlin: Springer; New Delhi: Hindustan Book Agency. xvi, 327 p. EUR 39.95 , 2006.

[23] Clémence Durvye. Evaluation techniques for zero-dimensional primary decomposition. *J. Symb. Comput.*, 44(9):1089–1113, 2009.

[24] Roberto Dvornicich and Carlo Traverso. Newton symmetric functions and the arithmetic of algebraically closed fields. Applied algebra, algebraic algorithms and error-correcting codes, Proc. 5th Int. Conference, AAECC-5, Menorca, Spain, 1987, Lect. Notes Comput. Sci. 356, 216-224, 1989.

[25] David Eisenbud. *Commutative algebra. With a view toward algebraic geometry.* Graduate Texts in Mathematics. 150. Berlin: Springer-Verlag. , 1995.

[26] Helaman R.P. Ferguson, David H. Bailey, and Steve Arno. Analysis of PSLQ, an integer relation finding algorithm. *Math. Comput.*, 68(225):351–369, 1999.

[27] William Fulton. *Intersection theory. 2nd ed.* Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. 2. Berlin: Springer. xiii, 470 p., 1998.

[28] André Galligo. A propos du théorème de preparation de Weierstrass. Fonctions de plusieurs Variables complexes, Sem. Francois Norguet, Oct. 1970 - Dec. 1973, Lect. Notes Math. 409, 543-579 (1974)., 1974.

[29] André Galligo and David Rupprecht. Irreducible decomposition of curves. *J. Symb. Comput.*, 33(5):661–677, 2002.

[30] Shuhong Gao. Absolute irreducibility of polynomials via Newton polytopes. *J. Algebra*, 237(2):501–520, 2001.

[31] Keith O. Geddes, Stephen R. Czapor, and George Labahn. *Algorithms for computer algebra.* Dordrecht: Kluwer Academic Publishers Group. XVIII, 585 p. , 1992.

[32] Patrizia Gianni, Barry Trager, and Gail Zacharias. Gröbner bases and primary decomposition of polynomial ideals. *J. Symb. Comput.*, 6(2-3):149–167, 1988.

[33] Marc Giusti, Joos Heintz, Jose Enrique Morais, and Luis M. Pardo. When polynomial equation systems can be "solved" fast? Cohen, Gérard (ed.) et al., Applied algebra, algebraic algorithms and error-correcting codes. 11th international symposium, AAECC-11, Paris, France, July 17-22, 1995. Proceedings. Berlin: Springer-Verlag. Lect. Notes Comput. Sci. 948, 205-231, 1995.

[34] Fernando Q. Gouvêa. *p-adic numbers. An introduction.* Universitext. Berlin: Springer-Verlag. vi, 284 p. DM 58.00 , 1993.

[35] Mark L. Green. Generic initial ideals. Elias, J. (ed.) et al., Six lectures on commutative algebra. Lectures presented at the summer school, Bellaterra, Spain, July 16–26, 1996. Basel: Birkhäuser. Prog. Math. 166, 119-186, 1998.

[36] G.-M. Greuel, G. Pfister, and H. Schönemann. SINGULAR 3-1-0 — A computer algebra system for polynomial computations. 2009. http://www.singular.uni-kl.de.

[37] Laurent Gruson, Robert Lazarsfeld, and Christian Peskine. On a theorem of Castelnuovo, and the equations defining space curves. *Invent. Math.*, 72:491–506, 1983.

[38] Laurent Gruson and Christian Peskine. Section plane d'une courbe gauche: Postulation. Enumerative geometry and classical algebraic geometry, Prog. Math. 24, 33-35 (1982)., 1982.

[39] Robin Hartshorne. Stable reflexive sheaves. *Math. Ann.*, 254:121–176, 1980.

[40] Robin Hartshorne. *Algebraic geometry. Corr. 3rd printing.* Graduate Texts in Mathematics, 52. New York-Heidelberg-Berlin: Springer- Verlag. XVI, 1983.

[41] Grete Hermann. Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. *Math. Ann.*, 95(1):736–788, 1926.

[42] Loo Keng Hua. *Introduction to number theory. Transl. from the Chinese by Peter Shiu.* Berlin-Heidelberg-New York: Springer-Verlag. XVIII, 572 p., 1982.

[43] Antoine Joux and Jacques Stern. Lattice reduction: A toolbox for the cryptoanalyst. *J. Cryptology*, 11(3):161–185, 1998.

[44] Erich Kaltofen. Fast parallel absolute irreducibility testing. *J. Symb. Comput.*, 1:57–67, 1985.

[45] Erich Kaltofen. Polynomial factorization 1982-1986. Computers and mathematics, Proc. Int. Conf., Stanford/CA (USA) 1986, Lect. Notes Pure Appl. Math. 125, 285-309 (1990)., 1990.

[46] Erich Kaltofen. Polynomial factorization 1987-1991. In I. Simon, editor, Proc. LATIN '92, 1992.

[47] Ravi Kannan, Arjen K. Lenstra, and László Lovász. Polynomial factorization and nonrandomness of bits of algebraic and some transcendental numbers. *Math. Comput.*, 50(181):235–250, 1988.

[48] Peter Kornerup and Robert T. Gregory. Mapping integers and Hensel codes onto Farey fractions. *BIT*, 23:9–20, 1983.

[49] Martin Kreuzer and Lorenzo Robbiano. *Computational commutative algebra. II.* Berlin: Springer. x, 586 p., 2005.

[50] Olav Arnfinn Laudal. A generalized trisecant lemma. Algebr. Geom., Proc., Tromso Symp. 1977, Lect. Notes Math. 687, 112-149 (1978)., 1978.

[51] Grégoire Lecerf. Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers . *Journal of Complexity*, 19(4):564–596, 2003.

[52] Grégoire Lecerf. Sharp precision in Hensel lifting for bivariate polynomial factorization. *Math. Comput.*, 75(254):921–933, 2006.

[53] Arjen K. Lenstra, Hendrik W.jun. Lenstra, and László Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261:515–534, 1982.

[54] Maplesoft. Maple - Math and Engeneering Software. see `http://www.maplesoft.com/`, 2009.

[55] Mathemagix. A free computer algebra system. Available at `http://www.mathemagix.org`, 2009.

[56] Emilia Mezzetti. Differential-geometric methods for the lifting problem and linear systems on plane curves. *J. Algebr. Geom.*, 3(3):375–398, 1994.

[57] Emilia Mezzetti and Irene Raspanti. A Laudal-type theorem for surfaces in $\mathbb{P}^4$. *Rend. Semin. Mat., Torino*, 48(4):529–537, 1990.

[58] David Mumford. *Lectures on curves on an algebraic surface.* Princeton, N.J.: Princeton University Press. XI, 200 p. , 1966.

[59] Phong Q. Nguên and Damien Stehlé. Floating-point LLL revisited. Cramer, Ronald (ed.), Advances in cryptology – EUROCRYPT 2005. 24th annual international conference on the theory and applications of cryptographic techniques, Aarhus, Denmark, May 22–26, 2005. Proceedings. Berlin: Springer. Lecture Notes in Computer Science 3494, 215-233, 2005.

[60] Emmy Noether. Ein algebraisches Kriterium für absolute Irreduzibilität. *Math. Ann.*, 85:26–33, 1922.

[61] Andrew Novocin and Mark Van Hoeij. Gradual sub-lattice reduction and a new complexity for factoring polynomials. to appear in Gradual sub-lattice reduction and a new complexity for factoring polynomials - LATIN 2010, Oaxaca : Mexico, 2010.

[62] Christian Okonek, Michael Schneider, and Heinz Spindler. *Vector bundles on complex projective spaces.* Progress in Mathematics. 3. Boston - Basel - Stuttgart: Birkhäuser. VII, 1980.

[63] Alexander Markowich Ostrowski. On multiplication and factorization of polynomials. I: Lexicographic orderings and extreme aggregates of terms. *Aequationes Math.*, 13:201–228, 1975.

[64] Franz Pauer. On lucky ideals for Gröbner basis computations. *J. Symbolic Comput.*, 14(5):471–482, 1992.

[65] Jean-Francois Ragot. *Sur la factorisation absolue des polynomes.* PhD thesis, Université de Limoges, France, 1997.

[66] Jean-Francois. Ragot. Probabilistic absolute irreducibility test for polynomials. *J. Pure Appl. Algebra*, 172(1):87–107, 2002.

[67] Margherita Roggero. Lifting problem for codimension two subvarieties in $\mathbb{P}^{n+2}$: border cases. Herzog, Jürgen (ed.) et al., Geometric and combinatorial aspects of commutative algebra. Papers based on lectures delivered at the international conference on commutative algebra and algebraic geometry, Messina, Italy, June 16–20, 1999. New York, NY: Marcel Dekker. Lect. Notes Pure Appl. Math. 217, 309-326, 2001.

[68] David Rupprecht. Semi-numerical absolute factorization of polynomials with integer coefficients. *J. Symb. Comput.*, 37(5):557–574, 2004.

[69] Wolfgang M. Schmidt. *Equations over finite fields. An elementary approach.* Lecture Notes in Mathematics. 536. Berlin-Heidelberg-New York: Springer-Verlag. IX , 1976.

[70] Rolf Schneider. *Convex bodies: the Brunn-Minkowski theory.* Encyclopedia of Mathematics and Its Applications. 44. Cambridge: Cambridge University Press. xiii, 490 p. , 1993.

[71] Claus Peter Schnorr. Fast LLL-type lattice reduction. *Inf. Comput.*, 204(1):1–25, 2006.

[72] Andrew J. Sommese and Jan Verschelde. Numerical homotopies to compute generic points on positive dimensional algebraic sets. *J. Complexity*, 16(3):572–602, 2000.

[73] Andrew J. Sommese, Jan Verschelde, and Charles W. Wampler. Numerical decomposition of the solution sets of polynomial systems into irreducible components. *SIAM J. Numer. Anal.*, 38(6):2022–2046, 2001.

[74] Andrew J. Sommese and Charles W. Wampler. Numerical algebraic geometry. Renegar, James (ed.) et al., The mathematics of numerical analysis. 1995 AMS-SIAM summer seminar in applied mathematics, July 17–August 11, 1995, Park City, UT, USA. Providence, RI: American Mathematical Society. Lect. Appl. Math. 32, 749-763, 1996.

[75] Peter Stevenhagen and Hendrik W.jun Lenstra. Chebotarëv and his density theorem. *Math. Intell.*, 18(2):26–37, 1996.

[76] Rosario Strano. Sulle sezione iperpiane dele curve. *Milan Journal of Mathematics*, 57(6):125–134, 1987.

[77] Alfonso Tortora. On the lifting problem in codimension two. *Matematiche*, 52(1):41–51, 1997.

[78] Barry Trager. *On the integration of algebraic functions*. PhD thesis, 1985.

[79] Barry Trager. Good reduction of curves and applications. Meeting on Computer and Commutative Algebra (COCOA II), 1989.

[80] Mario Valenzano. Bounds on the degree of two-codimensional integral varieties in projective space. *J. Pure Appl. Algebra*, 158(1):111–122, 2001.

[81] Joachim von zur Gathen and Jürgen Gerhard. *Modern computer algebra. 2nd ed.* Cambridge University Press, 2003.

[82] Franz Winkler. A p-adic approach to the computation of Gröbner bases. *J. Symbolic Comput.*, 6(2-3):287–304, 1988. Computational aspects of commutative algebra.

[83] Chee Keng Yap. *Fundamental problems of algorithmic algebra.* Oxford: Oxford University Press. xvi, 511 p., 2000.

[84] Umberto Zannier. On the reduction modulo p of an absolutely irreducible polynomial $f(x, y)$. *Arch. Math.*, 68(2):129–138, 1997.

Algorithmes de Factorisation de Polynomes et de Décomposition de Courbes

Résumé

Les courbes algébriques affines sont un outil qui est appliqué dans plusieurs domains, par example le CAGD. Elles sont définies par des polynômes, mais souvent elles ont plusieurs composantes irréductibles distinctes. Dans cette thèse on développe des algorithmes efficaces pour la décomposition d'une courbe definie par des polynômes rationelles.

Dans la première partie on présente un algorithme de factorisation absolue pour polynômes en deux variables (problème equivalent à la décomposition de courbes dans le plan). On part de l'algorithme existant TKTD et on améliore la définition de l'extension de corps nécessaire à la factorisation, utilisant des techniques modulaires et l'algorithme LLL pour identifier un nombre algébrique de son approximation p-adique.

Dans la deuxième partie on passe au problème de décomposer une courbe dans l'espace tridimensionel: l'équivalent de la factorisation pour le cas du plan est la décomposition primaire d'un idéal pour le cas des 3 dimensions. D'abord on montre des bornes sur les degrées des surfaces qui séparent les différentes composantes, utilisant des résultats classiques de géometrie algébrique, comme le "Lifting problem" ou la regularité de Castelnuovo-Mumford. Après, on considère un algorithme de décomposition classique, mais pas efficace du point de vue computationel, auquel on applique les techniques modulaires. On obtient un algorithme modulaire qui donne la fonction d'Hilbert des composantes réduites de la courbe.

Les deux algorithmes principales ont été testés sur plusieurs examples et comparés avec le temps d'exécution d'autres logiciels.

Polynomial Factorization and Curve Decomposition Algorithms

Abstract

Affine algebraic curves are a tool applied in different fields, for instance CAGD. They are defined using polynomials, but they often have several different irreducible components. In this thesis we develop efficient algorithms to decompose a curve defined by rational polynomials.

In the first part we present an absolute factorization algorithm for bivariate polynomials (this problem is equivalent to the decomposition of a curve in the plane). We start from the existing algorithm TKTD and we improve the definition of the algebraic extension needed for the factorization, using modular techniques and the LLL algorithm to identify an algebraic number form its p-adic approximation.

In the second part we pass to the problem of decomposing a curve in the three-dimensional space: the corresponding technique of the factorization for the case of the plan is the primary decomposition of an ideal for the three-dimensional case. At first, we show some bounds on the degrees of the surfaces separating the different components, using some classical results of algebraic geometry, as the "Lifting problem" or the Castelnuovo-Mumford regularity. After this, we apply consider a classical algorithm of decomposition, which is not efficient for computations, and we apply on it the modular techniques. We obtain a modular algorithm giving the Hilbert function for the reduced components of the curve.

The two main algorithms were tested on several examples and compared with the executions times of other softwares.