Modular absolute decomposition of equidimensional polynomial ideals

Cristina Bertone*

December 24, 2010

Abstract

In this paper, we present a modular strategy which describes key properties of the absolute primary decomposition of an equidimensional polynomial ideal defined by polynomials with rational coefficients. The algorithm we design is based on the classical technique of elimination of variables and colon ideals and uses a tricky choice of prime integers to work with. Thanks to this technique, we can obtain the number of absolute irreducible components, their degree, multiplicity and also the affine Hilbert function of the reduced components (namely, their initial ideal w.r.t. a degree-compatible term ordering).

Introduction

In this paper we design an algorithm whose aim is quite simple to state:
Given a set of polynomial rational equations which define an equidimensional algebraic set $\mathscr{W}$ of $\mathbb{C}^n$, we would like to get as many information as possible on the *irreducible components* of this algebraic set.

We can rephrase the problem in algebraic language: given an ideal (with suitable hypothesis on its dimension) in the polynomial ring over $\mathbb{C}[\mathbf{X}]$ defined by rational generators, find all the possible information about its primary components.

The problem is really simple to state and many authors looked for efficient strategies to get the irreducible decomposition of an algebraic set: one can see for instance [8] and the references therein to have an overlook of the different techniques. In many Computer Algebra Systems (CAS for short) you can find routines computing the primary decomposition of an ideal: the underlying algorithm is often the one described in [13]. Nevertheless, the problem is really challenging since the existing algorithms and implementations often focus on particular cases, e.g 0-dimensional ideals (see for instance [10]); for more general situations, also the best implemented algorithms (for instance, the ones in [4] or [13]) may have unsatisfying time of execution and there may be problems of memory allocation. In fact, the computations required to a personal computer to find a primary decomposition are often quite heavy.
Our aim is to design an algorithm concerning the decomposition of an ideal which can give an output in a reasonable time and with a limited use of memory.

The main computational tool that we use are modular computations, taking this technique from the absolute factorization algorithm for bivariate polynomials presented in [3].
Recent papers about decomposition of algebraic sets (see for instance [12], [21]) focus on getting

*Written with the support of the PRIN project "'Geometria delle varieta' algebriche e dei loro spazi di moduli" funds (co-financed by the MIUR, cofin 2008).

information about the irreducible components from a generic section with a linear space, namely they bring back the problem to the study of a 0-dimensional ideal.
In this paper we will bring back the problem of computing a primary decomposition to the problem of computing an absolute factorization; this technique is in some sense "classical" ([16]), but not very exploited because not efficient from the computational point of view; a powerful improvement of this technique is in [4], where the authors avoid the use of *generic* projections in order to compute the equidimensional isoradical decomposition of an ideal, using as coefficient ring $\mathbb{Q}$ or a finite field of positive characteristic. Our approach is instead to use generic projections (by a generic change of variables and projections on coordinate linear spaces) and exploit modular computations to move around the computational difficulties, preserving a lot of data concerning the absolute primary decomposition of the ideal. The output of our algorithm will not be the complete primary decomposition of the given ideal, but it will return information concerning the components, such as number, degree, multiplicity and, for reduced components, the affine Hilbert function.

In Section 1 we will show that once known information about one of the primary components of the ideal, the same is known for other components too. We simply rephrase the definition of "conjugacy" for absolute factors of a multivariate polynomial with rational coefficients (see [5], Lemma 9.0.8), for primary components of an ideal generated by polynomials with rational coefficients. Degree, multiplicity and affine Hilbert function are "invariant by conjugacy", so if we obtain this information about a primary component, we actually have the same information for all the primary components in its "conjugacy class", avoiding to repeat computations.

In Section 2 we show that, fixed an algebraic extension $\mathbb{L}$ of $\mathbb{Q}$, there are infinite prime integers that implicitly define a homomorphism from $\mathbb{L}$ to $\mathbb{Z}/p\mathbb{Z}$ (more precisely, an inclusion of $\mathbb{L}$ in $\mathbb{Q}_p$, Lemma 2.3). This means that with a careful choice of a prime p, we can reduce the coefficients of a polynomial in $\mathbb{L}[\mathbf{X}]$ modulo p. Furthermore, infinite prime numbers preserve interesting properties of an ideal in $\mathbb{L}[\mathbf{X}]$, namely the initial ideal with respect to some degree-compatible term ordering and, as a consequence of this, the affine Hilbert function.
Summing up, we can choose a prime p which allows modular computations in $\mathbb{L}$ (we can choose it using Lemma 2.3). Only a finite number of primes p does not preserve the properties of the primary components we are interested in, so we can assume that we are avoiding them by taking a “generic” prime p.

In Section 3 we present the exact strategy to obtain the prime components of an ideal $\mathfrak{a}$. This technique is mainly based on elimination of variables, in order to bring back the problem of primary decomposition to a problem of factorization. This strategy was first investigated by Grete Hermann in [16] and it is similar to the splitting techniques presented in [4], but we present it completely for lack of an accessible reference on the whole strategy. Nevertheless, the technique of Section 3 is not efficient from a computational point of view: first of all, projections are actually computed with a generic change of coordinates and an elimination of variables performed by a Groebner Basis; then, in order to obtain the reduced primary components, we compute a colon ideal; this is performed again by an elimination Groebner Basis.

In Section 4 we try to gain in computational efficiency, even if we “lose” the exactness of Section 3. We will apply the modular results of Section 2 on the exact algorithms of Section 3. We compute projections, factorizations and colon ideals modulo well-chosen prime integers; we do not get the reduced primary components, but we obtain an algorithm (Algorithm 3) which can compute the initial ideal of the reduced components of $\mathfrak{a}$ and give information about the non-reduced components.

Finally, in Section 5, we test our strategy on a simple example, a complete intersection ideal in 3 variables, getting the output of Algorithm 3 in a really reasonable time. The same ideal could not be decomposed by other CAS in 1 hour (because of problems with memory allocation); obviously the comparison between our strategy and implemented primary decomposition algorithms is

not complete, since Algorithm 3 does not return the absolute primary decomposition of the input ideal. However this comparison enlightens promising performances of our strategy and this can be a starting point for designing an efficient primary decomposition algorithm.

Notations

In what follows, we will work in a polynomial ring R with coefficients in a field $\mathbb{K}$ of characteristic 0: $R = \mathbb{K}[X_1, \ldots, X_n] = \mathbb{K}[\mathbf{X}]$. We will precise, when needed, if $\mathbb{K} = \mathbb{Q}$, $\mathbb{Q}(\alpha)$ or $\mathbb{C}$.

Given an ideal $\mathfrak{a} \subseteq R$ we will consider its zero set in $\mathbb{C}^n$: $\mathscr{W} = V(\mathfrak{a}) = \{P \in \mathbb{C}^n | f(P) = 0 \forall f \in \mathfrak{a}\}$.

1 Affine Hilbert Function and Conjugacy

In this section we introduce the main definitions concerning the primary decomposition and the affine Hilbert function of an ideal $\mathfrak{a} \subseteq R$.
We show that some of the primary components of an ideal $\mathfrak{a}$ are very "similar" to each other, in the sense that given a set of generators for a primary component, we can get a set of generators for another primary component by means of *conjugacy*, just like we do for the absolute factors of a polynomial with rational coefficients ([5], Lemma 9.0.8). This allows us to avoid repeating the computation of the affine Hilbert function for the conjugate components, since it is invariant by conjugacy.

For all the definitions and properties concerning primary decomposition, the main reference is [1], Chapter 4.

Definition 1.1. *A proper ideal $\mathfrak{q}$ in a ring R is* primary *if the following condition holds:*

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

Every prime ideal is obviously primary.

Proposition 1.2 ([1], 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 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:*

$$\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{q}_i. \tag{1.1}$$

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 (1.1) is said to be minimal*. Any primary decomposition can be reduced to a minimal one (see [1], page 52).*

Since we assume to work in a polynomial ring R with coefficients in a field, a minimal primary decomposition always exists.

The factorization of a multivariate polynomial and the primary decomposition of a polynomial ideal are very close to each other: indeed, the primary decomposition of a principal ideal corresponds

to computing the absolute factorization of the generator of the ideal. So we can look at the factorization of a multivariate polynomial as a particular case of primary decomposition.
Thanks to this similarity, it is natural to extend the definition of *degree* and *multiplicity* of a factor to a primary component. We can define them through the *affine Hilbert function* ([17], Section 5.6):

Definition 1.4. *Let $\mathfrak{a}$ be an ideal in the polynomial ring R 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 $\langle R_{\leq i}\rangle$ 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 $R/\mathfrak{a}$.

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

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

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

From Definition 1.4, it is natural to define the affine Hilbert series, polynomial, dimension and the affine regularity index of $R/\mathfrak{a}$. The definitions are similar to the analogous for the homogeneous case; for all these definitions and their properties, we refer to [17], Section 5.6.

Definition 1.5. *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 say "dimension and degree of $\mathfrak{a}$", meaning the dimension and 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 algebraic definition, which corresponds to the intuitive idea that the multiplicity counts "how many times" the primary component is repeated.

Definition 1.6. *[[2], Definition 10] Let $\mathfrak{q} \in R$ be a $\mathfrak{p}$-primary ideal. Then the* multiplicity *of $\mathfrak{q}$, $\mathrm{mult}(\mathfrak{q}_i)$, in $\mathfrak{p}$ is $\deg(\mathfrak{p})/\deg(\mathfrak{q})$.*

We will often talk about the multiplicity of a primary component, implying that it is the multiplicity in its radical.

We now briefly recall how to explicitly compute the affine Hilbert function.

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

$$\mathbf{X}^I \preceq \mathbf{X}^J \Rightarrow \deg \mathbf{X}^I \leq \deg \mathbf{X}^J.$$

Once fixed a term ordering $\preceq$ on $\mathbb{T}^n$, for a polynomial $g \in \mathbb{K}[\mathbf{X}]$, we denote with $LM_{\preceq}(g)$ (or simply $LM(g)$ if there is no ambiguity) the maximal monomial with respect to $\preceq$ appearing in g with non-zero coefficient.
In the following Proposition, $HF_{R/\mathfrak{b}}$ is the Hilbert function for a homogeneous ideal.

Proposition 1.7. *Let $\preceq$ be a degree compatible term ordering on $\mathbb{T}^n$. For every $i \in \mathbb{Z}$, we have $HF^a_{R/\mathfrak{a}}(i) = \sum_{j=0}^{i} HF_{R/LM_{\preceq}(\mathfrak{a})}(j)$. In particular, we have $HF^a_{R/\mathfrak{a}}(i) = HF^a_{R/LM_{\preceq}(\mathfrak{a})}(i)$ for all $i \in \mathbb{Z}$.*

Proof. See [17], Proposition 5.6.3. □

Proposition 1.7 gives us the practical way to compute the affine Hilbert function of $\mathfrak{a}$: chosen a degree compatible term ordering $\preceq$, we can compute the initial ideal of $\mathfrak{a}$ and then we count the number of elements in the vector space $R/LM_{\preceq}(\mathfrak{a})(j)$ for every $j \leq i$.

We now show with a few lemmas that, given an ideal $\mathfrak{a}$ defined by polynomials with rational coefficients, the relation of the primary decomposition on $\mathbb{Q}[\mathbf{X}]$ and the primary decomposition on $\mathbb{C}[\mathbf{X}]$ is similar to the relation between a rational and an absolute factorization of a multivariate polynomial with rational coefficients (as shown in [5], Lemma 9.0.8). In other words, there is a conjugacy relation among some of the primary components.

Definition 1.8. *Consider $\mathfrak{a}$ ideal in $\mathbb{C}[\mathbf{X}]$ defined by a set of polynomials with rational coefficients. Let $\mathfrak{a} = \bigcap_{j=1}^{s} \mathfrak{q}_i, \mathfrak{q}_i \in \mathbb{Q}[\mathbf{X}]$ be the* rational primary decomposition *of $\mathfrak{a}$; $\mathfrak{q}_i$ (resp. $V(\mathfrak{q}_i)$) is a* rational primary component *of $\mathfrak{a}$ (resp. of $V(\mathfrak{a})$).*
We then consider a primary decomposition in $\mathbb{C}[\mathbf{X}]$ of each rational primary component $\mathfrak{q}_i$:

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

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

Consider a non-pure rational component $\mathfrak{q}_i$ of an ideal $\mathfrak{a} \subseteq R$. Let $\mathbb{L}_i$ be the smallest (w.r.t. the degree of extension on $\mathbb{Q}$) normal algebraic extension of $\mathbb{Q}$ such that $\mathfrak{q}_i^{(1)}$ has a set of generators in $\mathbb{L}_i[\mathbf{X}]$; assume that $\mathbb{L}_i = \mathbb{Q}(\alpha_i)$ and we denote with $f_j(\alpha_i, \mathbf{X})$ a polynomial in the chosen set of generators of $\mathfrak{q}_i$; indeed, we can think of such a generator as a polynomial in $\mathbb{Q}[Z, \mathbf{X}]$ with Z evaluated in α_i. Consider the Galois group of $\mathbb{L}_i$ over $\mathbb{Q}$, $\mathcal{G}_i = Gal(\mathbb{L}_i/\mathbb{Q})$.

For every $\sigma \in \mathcal{G}_i$, 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

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

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; furthermore it is straightforward that the ideal $\sigma(\mathfrak{q}_i^{(1)})$ is $\sigma(\mathfrak{p}_i^{(1)})$-primary. Finally, if $\tau, \sigma \in \mathcal{G}_i$, $\tau \neq \sigma$, 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 $\overline{\mathbb{Q}}[\mathbf{X}]$.

Lemma 1.9. *Consider $\mathfrak{q}_i$ a non-pure rational component of $\mathfrak{a} \subseteq \mathbb{C}[\mathbf{X}]$ defined by polynomials with rational coefficients, $\mathbb{L}_i$ the smallest normal algebraic extension of $\mathbb{Q}$ such that $\mathfrak{q}_i^{(1)}$ has a set of generators in $\mathbb{L}_i[\mathbf{X}]$, $\mathcal{G} = Gal(\mathbb{L}_i/\mathbb{Q})$. The minimal primary decomposition of $\mathfrak{q}_i$ is*

$$\mathfrak{q}_i = \bigcap_{\sigma \in \mathcal{G}_i} \sigma\left(\mathfrak{q}_i^{(1)}\right), \tag{1.2}$$

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

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

Furthermore, it is a minimal primary decomposition. Indeed, 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 $\sigma \in \mathcal{G}$, 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 $\sigma(\mathfrak{q}_i^{(1)})$.

Using [1], Exercises 12 and 13 of Chapter 5, if we consider the associated primes and the natural homomorphism $\mathbb{Q}[\mathbf{X}] \to \mathbb{L}_i[\mathbf{X}]$, then the set of prime ideals $\{\mathfrak{p}_{ij}\}$ is the same as the set of prime ideals of $\mathbb{L}_i[\mathbf{X}]$ whose contraction is $\mathfrak{p}_i$. Then $\mathcal{G}$ acts transitively on the set $\{p_i^{(j)}\}_{j=1,\dots,r_i}$, that is $\{p_i^{(j)}\}_{j=1,\dots,r_i} = \{\sigma(\mathfrak{p}_i^{(1)})\}_{\sigma\in\mathcal{G}}$.

So $\bigcap_{\sigma\in\mathcal{G}} \sigma\left(\mathfrak{q}_i^{(1)}\right)$ is a minimal primary decomposition of $\mathfrak{q}_i$; since $\mathfrak{q}_i$ is a primary ideal, all its primary components in $\mathbb{L}_i[\mathbf{X}]$ have same dimension and there are no embedded components, so its primary decomposition is unique and is exactly the one in (1.2). □

Lemma 1.10. *Consider $\mathfrak{a} \subseteq \mathbb{C}[\mathbf{X}]$, defined by a set of polynomials with rational coefficients, with no embedded components. Then the minimal primary decomposition of $\mathfrak{a}$ is*

$$\mathfrak{a} = \bigcap_{i=1}^{r} \left(\bigcap_{\sigma\in\mathcal{G}_i} \sigma\left(q_i^{(1)}\right) \right). \tag{1.3}$$

Proof. Since the ideals $\sigma\left(q_i^{(1)}\right)$ are primary, we just need to show that the decomposition is minimal.

Condition 1 of Definition 1.3 about minimality is straightforward from Lemma 1.9.

For what concerns Condition 2, we just have to point out that if there is $\tilde{\mathfrak{p}}$ associated to two different primary components of $\mathfrak{a}$ in $\mathbb{C}[\mathbf{X}]$, $\sigma\left(q_i^{(1)}\right)$, $\sigma \in \mathcal{G}_i$, and $\tau\left(q_j^{(1)}\right)$, $\tau \in \mathcal{G}_j$, then we would have two associated primes of the rational primary decomposition included in one other or equal. But this contradicts the fact that $\mathfrak{a}$ has no embedded components and the minimality of the rational primary decomposition of $\mathfrak{a}$. □

Up to relabeling the automorphisms of $Gal(\mathbb{L}_i/\mathbb{Q})$, we can rewrite (1.3) as

$$\mathfrak{a} = \bigcap_{i=1}^{r} \left(\bigcap_{j=1}^{r_i} \mathfrak{q}_i^{(j)} \right), \tag{1.4}$$

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

Definition 1.11. *The primary decomposition (1.4) is the* absolute primary decomposition *of $\mathfrak{a}$ and for i such that $r_i \geq 2$, we say that $\mathfrak{q}_i^{(j)}$ (resp. $V(\mathfrak{q}_i^{(j)})$) is an* absolute component *of $\mathfrak{a}$ (resp. of $V(\mathfrak{a})$).*

If $\mathfrak{q}_i = \bigcap_{j=1}^{r_i} \mathfrak{q}_i^{(j)}$, we say that $\mathfrak{q}_i^{(j)}$ and $\mathfrak{q}_i^{(j')}$ are *conjugate*, and that $\{\mathfrak{q}_i^{(j)}\}_{j=1,\dots,r_i}$ is a *conjugacy class*. Any number or property of an absolute component is *invariant by conjugacy* if it is the same for all the absolute components in the same conjugacy class.

From now on we will focus on a particular kind of ideals, *equidimensional* ones.

Definition 1.12. *An ideal $\mathfrak{a}$ (resp. an algebraic set $\mathscr{W} \subseteq \mathbb{C}^n$) is* equidimensional *if all of its primary components (resp. all of its irreducible components) have the same dimension.*

Thanks to [1], Corollary 4.11, if $\mathfrak{a}$ is equidimensional, all of its primary components are uniquely determined and so in this case the primary decomposition is unique.

Furthermore, there is a wide class of ideals which are equidimensional: if we consider a complete intersection ideal $\mathfrak{a} \in R$ generated by $n - c$ polynomials, it is equidimensional. This can be seen as a consequence of the Affine Dimension Theorem ([15], Chapter I, Proposition 7.1).

We can finally fix our purpose.

Given a non-prime equidimensional ideal $\mathfrak{a} \subseteq \mathbb{C}[\mathbf{X}]$, generated by polynomials with rational coefficients, we write its primary decomposition as in (1.4). Then for every rational primary component $\mathfrak{q}_i$ of $\mathfrak{a}$, we would like to find the numbers r_i, $\deg(\mathfrak{q}_i^{(1)})$and $\mathrm{mult}(\mathfrak{q}_i^{(1)})$.
If $\mathrm{mult}(\mathfrak{q}_i^{(1)}) = 1$ (the primary component is reduced, and so it is prime) then we would also like to compute the affine Hilbert function of $R/\mathfrak{q}_i^{(1)}$.

Remark 1.13. *Thanks to Lemma 1.10, all the information concerning the primary component $\mathfrak{q}_i^{(1)}$ (such as degree, multiplicity and affine Hilbert function if the component is prime) are the same for all the conjugate components $\sigma(\mathfrak{q}_i^{(1)})$, $\sigma \in Gal(\mathbb{L}_i/\mathbb{Q})$, since we actually compute them by an initial ideal, which is invariant by conjugacy.*

2 Algebraic extensions of $\mathbb{Q}$ and modular computations

We are interested in preserving some properties of an ideal $\mathfrak{a}$ in $R = \mathbb{L}[\mathbf{X}]$ ($\mathbb{L}$ is a normal algebraic extension of $\mathbb{Q}$) "modulo" a well-chosen prime integer p. First of all we need to establish how we can compute an algebraic number modulo a prime p and then we will see that in general the reduction modulo p of the coefficients of a polynomial ideal preserves the affine Hilbert function of the ideal itself.

Let $\mathfrak{a} = (f_1, \ldots, f_s) \subseteq \mathbb{L}[\mathbf{X}]$ 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 $\mathbb{Q}$.

In the definition of a reduction of $\mathfrak{a}$ modulo a *well-chosen* prime p, our aim is preserving some features of $\mathfrak{a}$.

We fix a set of generators $(f_1, \ldots, f_s)$ in $\mathbb{Q}(\alpha)[\mathbf{X}]$. We multiply each f_i with a scalar c_i such that $c_i \cdot f_i \in \mathbb{Z}[\alpha][\mathbf{X}]$ and the coefficients of $c_i \cdot f_i$ have g.c.d. (on the integers) equal to 1: we call such a set of generators in $\mathbb{Z}[\alpha][\mathbf{X}]$ *primitive*. We keep on writing f_i for $c_i \cdot f_i$.

We now consider a prime integer p such that $q(T)$ splits in $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ in the following way:

$$q(T) = S_1(T) \cdot S_2(T) \bmod p,\ \deg S_1(T) = 1, \deg S_2(T) = s - 1,\ \gcd(S_1(T), S_2(T)) = 1. \quad (2.1)$$

Thanks to Chebotarev's Density Theorem ([22]), we know that there are infinite prime integers p for which (2.1) holds.

Let β_p be the only root of $S_1(T)$ in $\mathbb{Z}/p\mathbb{Z}$, $0 \leq \beta_p \leq p - 1$: $S_1(\beta_p) = 0$. We then define the following map, from the ring $\mathbb{Z}[\alpha]$ of $\mathbb{Z}$ to the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$:

$$\begin{aligned} \psi_p : \mathbb{Z}[\alpha] &\to \mathbb{F}_p \\ \alpha &\mapsto \beta_p \\ a \in \mathbb{Z} &\mapsto a \mod p. \end{aligned} \quad (2.2)$$

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:

$$\begin{aligned} \psi_p : \mathbb{Z}[\alpha][\mathbf{X}] &\to R_p = \mathbb{F}_p[\mathbf{X}] \\ f = \sum_I a_I \mathbf{X}^I &\mapsto \tilde{f} = \sum_I \psi_p(a_I)\mathbf{X}^I. \end{aligned}$$

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

Remark 2.1. *Observe that the definition of $\tilde{\mathfrak{a}}$ is independent on the chosen set of generators of $\mathfrak{a}$: if $\mathfrak{a} = (f_1, \ldots, f_s) = (f'_1, \ldots, f'_l)$ then $(\tilde{f_1}, \ldots, \tilde{f_s}) = (\tilde{f'_1}, \ldots, \tilde{f'_l})$ as ideals in R_p.*

Example 2.2. *Consider the ideal*

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

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 $\tilde{\mathfrak{a}} = (3\,Y^2 + 14\,ZX, 3\,YX + 12\,Z, 2\,X^2 + 18\,Y)$.

We can choose a prime p satisfying (2.1) using the following lemma.

Lemma 2.3. *[[3], Lemma 12] Let $q(T) \in \mathbb{Z}[T]$ be a polynomial and p a prime number such that p divides $q(0)$, p does not divide the discriminant of $q(T)$ and $p > \deg(q(T))$.*
Then there exists a root in $\mathbb{Q}_p$ of $q(T)$, considered as a polynomial in $\mathbb{Q}_p[T]$.

We would like to understand in which cases computations modulo a prime integer p preserve the affine Hilbert function of the ideal $\mathfrak{a}$. From Proposition 1.7, we can bring back our problem about the choice of a prime p preserving the affine Hilbert function to the choice of a "good" p preserving the initial ideal (w.r.t. some term ordering) of $\mathfrak{a}$.

Assume that $(g_1, \ldots, g_s)$ is a Groebner Basis of $\mathfrak{a}$ w.r.t. $\preceq$, degree compatible term ordering, and that these polynomials are primitive; we now choose a prime p satisfying (2.1) for the minimal polynomial of α. Then, we define $\tilde{\mathfrak{a}} := (\tilde{g}_1, \ldots, \tilde{g}_s) \subseteq R_p$.

Proposition 1.7 gives a necessary condition for a prime integer p to preserve the affine Hilbert function of $\mathfrak{a}$: if computations modulo p preserve $HF^a_{R/\mathfrak{a}}$ then they also preserve $LM_{\preceq}(\mathfrak{a})$ with respect to a degree-compatible term ordering $\preceq$.

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

Lemma 2.4. *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 at least one 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. We can define the polynomial $\tilde{L}(T) = \sum_{j=0}^{s-1} a_j^{(\tilde{\imath})} T^j$.

If $\deg \tilde{L}(T) = 0$, $\tilde{L}(T) = L_{\tilde{\imath}}$ is an integer and there is only a finite number of ψ_p mapping $L_{\tilde{\imath}}$ to zero, because there is only a finite number of p's dividing it.

We can then assume that $d = \deg \tilde{L}(T) \geq 1$. We consider a prime p such that

$$\psi_p(L_{\tilde{\imath}}) = 0, \quad p \geq \|\tilde{L}(T)\|^s \|q(T)\|^d,$$

where $q(T)$ is the 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.
Observe that $\psi_p(L_{\tilde{i}}) = \tilde{L}(\beta_p) \mod p = 0$. This means that both $\tilde{L}(T)$ and $q(T)$ can be divided by $(T - \beta_p)$ modulo p. But since we chose $p \geq \|\tilde{L}(T)\|^s \|q(T)\|^d$, we can apply [23], Lemma 16.20: $\deg\left(\gcd(\tilde{L}(T), q(T))\right) \geq 1$.
Since $\deg \tilde{L}(T) < \deg q(T)$, this contradicts the fact that $q(T)$ is irreducible. □

Lemma 2.5. *Let $\mathfrak{a}$ be an ideal in $\mathbb{Q}(\alpha)[\mathbf{X}]$, $\preceq$ a term ordering and $G = \{g_1, \ldots, g_r\}$ a Groebner Basis of $\mathfrak{a}$ with respect to $\preceq$, p a prime integer satisfying (2.1) for the minimal polynomial of α.*
If ψ_p does not map to 0 any of the coefficients of the leading monomials 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 $\preceq$.

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 $LM(\tilde{g}) = \max_{i=1,\ldots,r}\{LM(\tilde{a}_i \tilde{g}_i)\}$, where the "max" is taken with respect to $\preceq$.

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 coefficients of the leading monomials of the polynomials in the Groebner basis, we immediately have $LM(\tilde{g}) \in (LM(\tilde{g}_1), \ldots, LM(\tilde{g}_s))$ and so $\tilde{G}$ is a Groebner Basis for $\tilde{\mathfrak{a}}$. □

Theorem 2.6. *Let $\mathfrak{a}$ be an ideal in $R = \mathbb{Q}(\alpha)[\mathbf{X}]$. 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 ordering $\preceq$ and consider the Groebner Basis $G = \{g_1, \ldots, , g_r\}$ of $\mathfrak{a}$. Thanks to Proposition 1.7, $HF^a_{R/\mathfrak{a}}(i) \neq HF^a_{R_p/\tilde{\mathfrak{a}}}(i)$ for some i only if the initial ideal of $\mathfrak{a}$ differs from $\tilde{\mathfrak{a}}$.
We apply Lemma 2.5: there is only a finite number of primes p such that the initial ideals of $\mathfrak{a}$ and $\tilde{\mathfrak{a}}$ are different. □

Corollary 2.7. *There is a finite number of prime integers p such that the affine Hilbert function and dimension of $\mathfrak{a}$ and $\tilde{\mathfrak{a}}$ differ. If $\mathfrak{a}$ is a primary component of some ideal, the same holds for the multiplicity of $\mathfrak{a}$ and $\tilde{\mathfrak{a}}$.*

3 An exact strategy: Elimination of Variables and Colon Ideals

In this section, we will present an exact technique, which combines elimination of variables, absolute factorization and computation of colon ideals and gives the primary decomposition of an ideal.

This technique is intuitive and immediate from the geometric point of view: the elimination of variables geometrically corresponds to projection on some linear space.

The use of projections reduces the problem of decomposing an algebraic set to a multivariate factorization; this was first showed at the beginning of the XX-th century (see [16]). After that, Seidenberg in [20] used a more rigorous formalism then Hermann's to establish which ideal operation can be actually computed, depending also on the features of the polynomial ring we are working on.
The computation of a colon ideal geometrically corresponds to take off the points of an algebraic set from another one. This relation between the "difference" of varieties and colon ideals is well-known too (see [7], Chapter 4, §4).

The strategy of elimination of variables and computation of quotient ideals is also used in [4]. The authors in [4] can move around the computational effort of using *generic* projections (in the sense of Definition 3.2) by using another powerful tool, which is the relation between flatness and variation of staircases. Thanks to the study of the flatness of the variation of the staircases, they can split the ideal according to the splitting of the projection, even if it is not a generic one; they repeat the process for the ideals obtained by splitting and at each step they have the dimension or the multiplicity of the ideals decreasing, so their algorithm terminates. The algorithm in [4] has different variants and can give the strict, isoradical and reduced equidimensional decomposition of a polynomial ideal in $\mathbb{Q}[\mathbf{X}]$ (see [4], Introduction, for the different kind of decompositions).
Unfortunately, even if in [4] the proofs are given for a field k, with suitable properties that $\overline{Q}$ has, the implementation of the algorithm in CoCoAdeals only with $\mathbb{Q}$ or a finite field as coefficient fields, so this algorithm is not used in a CAS for the computation of an absolute primary decomposition (see Section 5).

Although the basic idea of the technique we are going to use is well-known, for lack of a complete and accessible reference on the whole strategy relating the algebraic and geometrical point of view , we will present it in an exhaustive way.

The decomposition algorithm that we can obtain using these techniques (Algorithm 1) 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) we will modify this strategy giving up the exact computations in order to gain velocity in computations, but preserving some information about the irreducible and reduced components, namely their affine Hilbert Function.

First of all, we now investigate some properties of the projection of varieties. For the omitted proofs, see [21].

Definition 3.1. *A* linear projection *is a surjective affine map:*

$$\begin{aligned} &\pi : \mathbb{C}^n \to \mathbb{C}^m \\ &P = (x_1, \ldots, x_n) \in \mathbb{C}^n \mapsto (L_1(P), \ldots, L_m(P)) \quad \textit{with } L_i(\mathbf{X}) = a_{i_0} + \sum_{j=1}^{n} a_{i_j} X_j. \end{aligned} \tag{3.1}$$

In a similar way, we can define a linear projection to projective space, considering

$$\begin{aligned} &\pi_L : \mathbb{P}^n \setminus L \to \mathbb{P}^m \\ &P = [x_0 : x_1 : \ldots : x_n] \mapsto [L_0(P) : L_1(P) : \ldots : L_m(P)], \quad L_i(\mathbf{X}) = \sum_{j=0}^{n} a_{i_j} X_j. \end{aligned} \tag{3.2}$$

$L \subseteq \mathbb{P}^n$ *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* $\mathbb{P}^n$ *to* $\mathbb{P}^m$ *are* equivalent *if they have the same center* L*.*

We now consider a projection $\pi : \mathbb{C}^n \to \mathbb{C}^m$ and we restrict it to an equidimensional algebraic set $\mathscr{W}$ of $\mathbb{C}^n$ with dimension c. It is not always true that $\pi_{\mathscr{W}}$ is proper: for instance, the projection of

the hyperbola defined by the ideal $(XY-1)$ on the X-axis is the Y-axis without the origin; with this particular choice of the linear space to project on, the restriction of π to the hyperbola is not proper.

Proposition 3.2 ([21], Lemma 5.1)**.** *Let $\mathscr{W}$ be a closed algebraic set of $\mathbb{C}^n$ all of whose irreducible components are of dimension c. For a general linear projection $\pi : \mathbb{C}^n \to \mathbb{C}^m$, $m \geq c+1$, the map $\pi_{\mathscr{W}}$ is proper and generically one-to-one.*
In particular $\pi(\mathscr{W})$ is a closed algebraic set of $\mathbb{C}^m$ of degree equal to the degree of $\mathscr{W}$.

Corollary 3.3. *Let $\mathscr{W}$ be an equidimensional algebraic set of dimension c in $\mathbb{C}^n$. For a general projection $\pi : \mathbb{C}^n \to \mathbb{C}^{c+1}$, the following hold:*

1. *if $\mathscr{W}_i$ and $\mathscr{W}_j$ are two distinct irreducible components of $\mathscr{W}$, then $\pi(\mathscr{W}_i) \neq \pi(\mathscr{W}_j)$;*
2. *$\mathscr{W}$ is irreducible if and only if the polynomial defining $\pi(\mathscr{W})$ is absolutely irreducible;*
3. *if $D(T_1, \ldots, T_c)$ is the polynomial defining the projection $\pi(\mathscr{W})$ and we consider its absolute factorization $D = D_1^{m_1} \cdots D_s^{m_s}$, then s is exactly the number of distinct irreducible components of $\mathscr{W}$, m_i is the multiplicity of the component $\mathscr{W}_i$ and $\deg D_i$ its degree.*

We now assume that $\mathscr{W}$ is an equidimensional algebraic set of dimension c defined by the ideal $\mathfrak{a} \subseteq \mathbb{C}[\mathbf{X}]$, $\mathfrak{a} = (F_1, \ldots, F_r), F_i \in \mathbb{Q}[\mathbf{X}]$; we further assume that we performed a generic linear change of coordinates with integer coefficients; in this way we can consider the projections on linear spaces defined by equations of kind $X_i = 0$ to be generic.

We consider the projection $\pi_1 : \mathbb{C}^n \to H_1$, with H_1 the linear space of dimension $c+1$ defined by the equation $X_{c+2} = \cdots = X_n = 0$. We call $\mathcal{Z}_1$ the projection of the algebraic set $\mathscr{W}$ on H_1. This is a hypersurface in H_1 and its decomposition is equivalent to the absolute factorization of the multivariate polynomial $D_1(X_1, \ldots, X_{c+1}) \in \mathbb{Q}[\mathbf{X}]$ defining $\mathcal{Z}_1$ on the linear space H_1. Furthermore, the components of $\mathcal{Z}_1$ are in one-to-one correspondence with the irreducible components of $\mathscr{W}$.

If $D_1 = D_{11}^{m_1} \cdots D_{1s}^{m_s}, D_{1j}^{m_j} \in \mathbb{C}[\mathbf{X}]$, is the absolute factorization of D_1, each factor D_{1j} defines in $\mathbb{C}^n$ a ruled surface, a cylinder, containing the component $\mathscr{W}_j$.
Algebraically, thanks to the generic change of coordinates and to Corollary 3.3, if $\mathfrak{a} = \bigcap \mathfrak{q}_j$, then there is only one absolute factor D_{1j} in the absolute factorization of D_1 such that $D_{1j}^{m_j} \in \mathfrak{q}_j$. Furthermore, for $m < m_j$, $D_{1j}^{m} \notin \mathfrak{q}_j$.

We can then start considering the ideal $\mathfrak{a} + (D_{1j}^{m_j})$. But $V(\mathfrak{a} + (D_{1j}^{m_j}))$ contains not only the component $\mathscr{W}_j$, but also the points of the sets $V(D_{1j}^{m_j}) \cap \mathscr{W}_k$ for $k \neq j$.

Thinking of the corresponding varieties $V(\mathfrak{q}_i)$ and $V(D_{1j}^{m_j})$, we can classify the primary components of the ideal $\mathfrak{a} + (D_{1j}^{m_j})$ as follows:

- a primary component of dimension c, which is the primary component $\mathfrak{q}_i$ such that $D_j^{m_j} \in \mathfrak{q}_i$ (and in this case we write $i = j$). Obviously in this case $\mathfrak{q}_j + (D_{1j}^{m_j}) = \mathfrak{q}_j$ and $\mathfrak{p}_j + (D_{1j}) = \mathfrak{p}_j$;
- other primary components of dimension $< c$ when $V(\mathfrak{q}_i) \cap V(D_{1j}^{m_j})$ is non-empty and it does not contain the component $\mathscr{W}_j$.

Finally, the ideal $\mathfrak{a} + (D_{1j}^{m_j})$ defines the component $\mathscr{W}_j$ with some extra components of dimension $< c$. In order to avoid these extra components, we can repeat the same steps with $(n-c-1)$ more generic projections π_k from $\mathbb{C}^n$ onto the linear spaces H_k, defined by equations of kind $X_i = 0$, thanks to the chosen generic coordinates (see also Section 3.1 for more details). If we consider $\pi_k(\mathscr{W}) = \mathcal{Z}_k$, the polynomial defining $\mathcal{Z}_k$ on H_k is again a rational multivariate polynomial D_k in $c+1$ variables. We compute its absolute factorization and we obtain another cylinder containing $\mathscr{W}_j$, defined by the factor D_{kj}.

Actually, in the absolute factorizations of the polynomials D_k there may be several factors with the same degrees and multiplicity. For instance, this happens when one of the components $\mathscr{W}_j$ is a non-pure rational one (see Definition 1.8). This can give ambiguity in matching the factors of the polynomials D_k whose zero set contains the component $\mathscr{W}_j$.

In order to match the factors defining the cylinders containing the same component, we can look at the Hilbert dimension of the ideal $\mathfrak{a} + (\sum_{k=1}^{c+1}(D_{kj}^{m_j}))$. This dimension is c if and only if all of the sets $V(D_{kj}^{m_j})$ contain the same irreducible component of $\mathscr{W}$; this follows from Corollary 3.3, 1.

In order to find the correct matchings, we will not compute the Hilbert dimensions of the ideals $\mathfrak{a}+(\sum_{k=1}^{c+1}(D_{kj}^{m_j}))$ for every possible $(n-c)$-uple of factors; we will compute the Hilbert dimension only for the matchings such that all the factors D_{kj} have the same degree and multiplicity. Furthermore, we get an almost certain probabilistic check by considering a generic section with a linear space of dimension $n-c$: that is, we can look for the matchings such that the ideal $\mathfrak{a} + (\sum_{k=1}^{c+1}(D_{kj}^{m_j}))$ with $(n-c)$ variables evaluated in some integer values is zero-dimensional and nonempty (see Algorithm 2).

Once matched the absolute factors found through the projections, $\{D_{kj}\}_{j=1,\dots,c}$ (after re-indexing of the factors), the ideal

$$\mathfrak{a}_j := \mathfrak{a} + (\sum_{k=1}^{c+1}(D_{kj}^{m_j})) \tag{3.3}$$

is "almost" the primary ideal corresponding to the component $\mathscr{W}_j$: there are some embedded components left, which geometrically are in $\mathscr{W}_j \cap \mathscr{W}_l$, for $l \neq j$.

Lemma 3.4. *Consider $(n-c)$ projections π_i from $\mathbb{C}^n$ to $\mathbb{C}^{c+1}$, pairwise not equivalent. If there are points $P_1, P_2 \in \mathbb{C}^n$ such that*

$$\pi_i(P_1) = \pi_i(P_2) \quad \forall i = 1, \dots, n-c,$$

then $P_1 = P_2$.

Proof. We write $\pi_k(P) = (L_1^{(k)}(P), \dots, L_{c+1}^{(k)}(P))$ with $L_i^{(k)}(\mathbf{X}) = a_{i0}^{(k)} + \sum_{j=1}^n a_{ij}^{(k)} X_j$. Remark that since a projection is a surjective map, $L_i^{(k)} \neq L_j^{(k)}$, $1 \leq i < j \leq c+1$; furthermore, we will be interested in the matrix whose lines are the vectors $\left(a_{ij}^{(k)}\right)_{j=1,\dots,n}$ for $k = 1, \dots n-c, i = 1, \dots, c+1$. It is a matrix with $(n-c)(c+1)$ lines and n columns; since the chosen projections are pairwise non-equivalent, this matrix has maximal rank: $(n-c)(c+1) \geq n$ for all $0 \leq c \leq n-1$, so the considered matrix has rank n.

P_1 and P_2 have the same image under π_j if and only if $L_i^{(j)}(P_1) = L_i^{(j)}(P_2)$, $i = 1, \dots, c+1$. We obtain $(n-c)\cdot(c+1)$ equations of kind

$$\sum_{j=1}^n a_{ij}^{(k)}(x_j^{(1)} - x_j^{(2)}) = 0, \quad P_1 = (x_j^{(1)})_{j=1,\dots,n}, P_2 = (x_j^{(2)})_{j=1,\dots,n}.$$

The unique solution to this system of equations is the trivial one, since the matrix associated to the linear system is exactly $\left(a_{ij}^{(k)}\right)$ whose rank is n, and so we have that $P_1 = P_2$. □

Corollary 3.5. *Consider $\mathscr{W}$ equidimensional algebraic set of dimension c in $\mathbb{C}^n$ and $\mathscr{W}_1$ and $\mathscr{W}_2$ irreducible components of $\mathscr{W}$. If $P_1 \in \mathscr{W}_1$ and $P_2 \in \mathscr{W}_2$ are such that*

$$\pi_i(P_1) = \pi_i(P_2),$$

for $(n-c)$ generic projections $\pi_i : \mathbb{C}^n \to \mathbb{C}^{c+1}$, then $P_1 = P_2$ is a point in $\mathscr{W}_1 \cap \mathscr{W}_2$.

Thanks to Lemma 3.4 and the one-to-one correspondence between the components of $\mathscr{W}$ and the components of $\pi(\mathscr{W})$, for a general projection π, if we consider the ideal $\mathfrak{a}_j$ as in (3.3), $V(\mathfrak{a}_j)$ is $\mathscr{W}_j$; however the polynomials in $\mathfrak{a}_j$ vanish on the points of $\mathscr{W}_k \cap \mathscr{W}_l$, $l \neq j$, with multiplicity higher than $\mathrm{mult}(\mathscr{W}_j)$.

So, for the moment, we have an ideal such that its zero set contains the irreducible component $\mathscr{W}_j$ but there are some embedded components; we now show that the points of these embedded components are also contained in the zero set of the singular locus of $\mathfrak{a}_j$ (Definition 3.6).
Considering again primary decompositions, for what concerns $\mathfrak{a}_j$ we have that:

$$\mathfrak{a}_j = \mathfrak{a} + (\sum_{k=1}^{c+1}(D_{kj}^{m_j})) = \mathfrak{q}_j \cap (\bigcap_{i=1}^{v} \mathfrak{b}_i) \tag{3.4}$$

where $\mathfrak{b}_i$ is a primary ideal of dimension $< c$. Geometrically, the primary components $\mathfrak{b}_i$ correspond to the irreducible component of $\mathscr{W}_j \cap \mathscr{W}_k$, $j \neq k$. These components are in the *singular locus* of $R/\mathfrak{a}$.

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

Definition 3.6. *Let $\mathfrak{a}$ be an ideal in $R = \mathbb{K}[\mathbf{X}]$, $\mathbb{K}$ perfect field, $\mathfrak{a} = (f_1, \ldots, f_s)$. A prime ideal $\mathfrak{p}$ containing $\mathfrak{a}$ is in the* singular locus *of $R/\mathfrak{a}$ if the localization of $R/\mathfrak{a}$ 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 $R/\mathfrak{a}$.

Proposition 3.7 ([11], Corollary 16.20)**.** *Let $\mathfrak{a}$ be an ideal in $\mathbb{K}[\mathbf{X}]$, $\mathbb{K}$ perfect field, $\mathfrak{a}$ is equidimensional with dimension c, $\mathfrak{a} = (f_1, \ldots, f_s)$. Let J be the ideal generated by the $(n-c)\times(n-c)$-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 $\mathfrak{a}$;
- Compute $\{M_l\}$, the $(n-c)\times(n-c)$ minors of the jacobian matrix;
- The singular locus of $\mathfrak{a}$ is defined by (M_l).

We are then interested in considering $\mathfrak{a}_j$ and removing the "embedded" primary components which contains the singular locus of $\mathfrak{a}$. We can do this for the ideals $\mathfrak{a}_j$ containing a reduced component, that is the ones obtained from irreducible factors of multiplicity 1.

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 a single element f of R, we will simply write $(\mathfrak{a} : f)$ instead of $(\mathfrak{a} : (f))$.

Lemma 3.8 ([1], 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 3.9. *In the previous setting, if D_{ij} are factors of multiplicity one in the factorizations of the polynomials D_i, such $D_{ij} \in \mathfrak{q}_j$, $\mathfrak{a}_j = \mathfrak{a} + (\sum_{k=1}^{c+1}(D_{kj}))$ and M is a $(n-c)\times(n-c)$ minor of the Jacobian matrix of $\mathfrak{a}$, then $(\mathfrak{a}_j : M)$ is exactly $\mathfrak{p}_j$, the prime ideal defining the irreducible component $\mathscr{W}_j$ of $\mathscr{W} = V(\mathfrak{a})$.*

Proof. Consider the primary decomposition of $\mathfrak{a}_j$:

$$\mathfrak{a}_j = \mathfrak{a} + (\sum_{k=1}^{c+1}(D_{kj})) = \mathfrak{q}_j \cap (\bigcap_{i=1}^{v} \mathfrak{b}_i)$$

where $\mathfrak{q}_j$ is the only component of dimension c, while $\mathfrak{b}_i$ are embedded components of dimension $< c$. These embedded components correspond to the intersection of $\mathscr{W}_j$ with the other irreducible components of $\mathfrak{a}$. Furthermore, since the factors D_{kj} have multiplicity one in the factorizations of the D_i, this means (Corollary 3.3) that $\sqrt{\mathfrak{q}_j} = \mathfrak{q}_j$, that is $\mathfrak{q}_j$ is a prime component, so we can write $\mathfrak{p}_j$ for $\mathfrak{q}_j$.

This means that if M is an equation of the singular locus of $\mathfrak{a}$, then $M \in \mathfrak{b}_i$ for $i = 1, \ldots, v$ and so $(\mathfrak{b}_i : M) = (1)$. On the other hand, $\mathfrak{p}_j$ is the only primary (and prime) component of $\mathfrak{a}_j$ which does not contain the singular locus: so $(\mathfrak{p}_j : M) = \mathfrak{p}_j$.

So

$$\mathfrak{a}_j : M = (\mathfrak{p}_j : M) \cap \left(\bigcap_{i=1}^{v} (\mathfrak{b}_i : M) \right) = \mathfrak{p}_j.$$

□

Remark 3.10. *Proposition 3.9 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 $\mathfrak{a}_j = \mathfrak{a} + (\sum_{k=1}^{n}(D_{kj}^{m_j}))$, $m_j \geq 2$, we have that this ideal contains the singular locus of $\mathfrak{a}$, so $M \in \mathfrak{a}_j$ and (using Lemma 3.8), $(\mathfrak{a}_j : M) = (1)$.

For components of multiplicity > 1, we may "clean up" at least some of the embedded components of the ideal $\mathfrak{a}_j$ in the following way:

- *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 $\{\mathscr{W}_{i_1}, \ldots, \mathscr{W}_{i_v}\}$*
- *since we cannot 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 "clean" part of the points of the embedded components. For the remaining ones, for any component of multiplicity > 1 we should consider the absolute factors D_{1j} of D_1 not contained in this primary component, and compute again some "nested" colon ideals, starting from $\mathfrak{b}$, with respect to the D_{1j}.

3.1 Algorithms

In this section we will summarize the strategy of elimination of variables and colon ideals, writing down the main algorithm for primary decomposition (Algorithm 1) and an auxiliary one to match $(n-c)$-uples $D_{1j}^{m_j}, \ldots, D_{cj}^{m_j}$ (Algorithm 2).

In order to consider $(n-c)$ projections $\pi_i : \mathbb{C}^n \to \mathbb{C}^{c+1}$ (pairwise non-equivalent) and compute the polynomials D_i which is zero on $\pi_i(\mathscr{W})$, at the beginning of Algorithm 1 we perform a generic change of affine coordinates and then use projections on "coordinate" affine linear spaces, namely linear spaces defined by equations of kind $X_j = 0$. While in the previous section we used "H" for the coordinate affine linear space, we will now use "H" to denote the set of indexes of the variables X_j to eliminate to obtain the projection of the curve:

$$X_j = 0, \quad j \in H = \{j_1, \ldots, j_{n-c-1}\} \subseteq 1, \ldots, n = [n]. \tag{3.5}$$

We can always find $(n-c)$ sets of indexes H_i, $i = 1, \ldots, n-c$, such that $H_l \neq H_m$ for every $l \neq m$. If $H = \{j_1, \ldots, j_{n-c-1}\}$, we write $\{X_l\}_{l \in [n] \setminus H}$ for $\{X_{l_1}, \ldots, X_{l_{c+1}}\}$, with $[n] \setminus H = \{l_1, \ldots, l_{c+1}\}$.

The actual computation of the polynomial D_i is obtained by the computation of a Groebner Basis with respect to an elimination term ordering.
If we consider the set of indexes H as in (3.5), we can compute a Groebner Basis which eliminates from $\mathfrak{a}$ the variables X_j, $j \in H$; from now on we will denote such a Groebner Basis with $GB_{elim(H)}(\mathfrak{a})$, or, if we fix H_i, $i = 1, \ldots, n-c$, we simply write $GB_{elim(i)}(\mathfrak{a})$. Then D_i is the only generator of $GB_{elim(i)}(\mathfrak{a})$ such that

$$D_i \in GB_{elim(i)}(\mathfrak{a}) \cap \mathbb{Q}[X_l]_{l \in [n] \setminus H_i} \tag{3.6}$$

We will always assume that $H_1 = \{c+2, \ldots, n\}$.

In Algorithm 2, in order to match the absolute factors corresponding to the same component, we use the fact that if an algebraic set has dimension $< c$, then its general section with a linear space of dimension $(n-c)$ is empty; this means that if $\mathfrak{b}$ is an ideal of dimension $< c$, then the affine Hilbert Dimension of $\mathfrak{b}$ with $(n-c)$ variables evaluated in integer values is generically -1. Furthermore, thanks to the generic change of coordinates, we can evaluate the variables in 0.

Thanks to the results of Section 1, we can modify Algorithm 1 and 2 and avoid repeating the computations for conjugate primary components. We present the Algorithms without this for simplicity and also because they will not actually be used in this form.

Indeed, Algorithm 1 is exact, but in practice the computations are too heavy: the main computational difficulties are at Step 2 (because of the computation of the Groebner Basis), Step 3 (because of the multivariate absolute factorization) and Step 8 (because of the computation of the colon ideal) of Algorithm 1.

In the next section we show that we can perform all these computations modulo a well-chosen prime integer p, obtaining Algorithm 3. Its output is no more exact, in the sense that it does not return the ideals of the reduced components, but it returns information about the ideals of the reduced components, in particular their initial ideal and affine Hilbert functions.

This will be possible observing that the computations of the troublesome steps of Algorithm 1 are actually obtained through Groebner Basis and that a good choice of p preserves along the computations the initial monomials of the polynomials in the Groebner Basis and so the Hilbert functions of the ideals.

Algorithm 1: Exact Decomposition of an equidimensional algebraic set

Data: $\mathfrak{a} \in \mathbb{Q}[X_1, \ldots, X_n]$, $\mathfrak{a}$ of pure dimension c

Result: The number of irreducible components, their degrees and multiplicities.
If the multiplicity of the component $\mathscr{W}_j$ is 1, a system of generators of the ideal $I(\mathscr{W}_j)$; if the multiplicity of the component is ≥ 2, the equations of $(n-c)$ hypersurfaces "isolating" the component from the other ones.

Preprocessing: Perform a generic affine change of coordinates on the generators of $\mathfrak{a}$;
Compute $(n-c)$ polynomials, eliminating from $\mathfrak{a}$ the set of variables corresponding to the set of indexes H_i, $i = 1, \ldots, n-c$: D_i is the only generator of $GB_{elim(i)}(\mathfrak{a})$ with the property (3.6), $i = 1, \ldots, n-c$;
Perform the absolute factorization of D_i, $i = 1, \ldots, n-c$
$D_i = D_{i1}^{m_1} \cdots D_{is}^{m_s}, \quad i = 1, \ldots, n-c$;
Match the D_{ij}'s through Algorithm 2 in such a way that (after re-numbering of the factors) $\mathfrak{a}_j = \mathfrak{a} + (\sum_{k=1}^{n-c}(D_{kj}))$ contains the component $\mathscr{W}_j$;
Compute the Jacobian matrix of $\mathfrak{a}$ and a minor of size $(n-c) \times (n-c)$, M ;
for i *from* 1 *to* s **do**
    if m_i *is 1* **then**
        Compute $\mathfrak{a}_j^{(M)}$ the quotient ideal of $\mathfrak{a}_j$ with M: $\mathfrak{a}_j^{(M)} := \mathfrak{a}_j : (M)$;
    end
end
Return:
for $j = 1, \ldots, s$: $\deg D_{1j}$ degree of the component, m_j multiplicity of the component;
if $m_j \geq 2$, $\mathfrak{a}_j$ ideal isolating the component;
if $m_j = 1$, $\mathfrak{a}_{ij}^{(M)} = I(\mathscr{W}_j)$.

Algorithm 2: Matching of factors through Hilbert Dimension

Data: $\mathfrak{a}$ and the absolute factors $\{D_{ij}\}_{\substack{i=1,\dots,n-c\\ j=1,\dots,s}}$, obtained at Step 3 of Algorithm 1.

Result: After relabeling the polynomials for the index j, $L := [(D_{ij}^{m_j})_{i=1,\dots,n-c})]_{j=1,\dots,s}$ with $V(\mathfrak{a} + (\sum_{i=1}^{n}(D_{ij})))$ containing the component $\mathscr{W}_j$ of $V(\mathfrak{a})$ for every $j = 1, \dots, s$.

1 $L :=$ empty list;
2 **for** j *from* 1 *to* s **do**
3 Consider a $(n-c)$-uple $(D_{ij})_{i=1,\dots,n-c}$ s.t. $\deg D_{ij} = d_j$ and $m_{ij} = m_j \forall i$;
4 Compute the Hilbert Dimension h of the ideal $\mathfrak{a} + (\sum_{i=1}^{n}(D_{ij}))$ with $(n-c)$ variables evaluated in 0;
5 **if** *h=0* **then**
6 add the $(n-c)$-uple $(D_{ij}^{m_j})$ to the list L;
7 **else**
8 go back to Step 3 and change $(n-c)$-uple;
9 **end**
10 **end**
11 Re-number the factors of D_i in such a way that the $(n-c)$-uples in L are of the form $(D_{1j}^{m_j}, \dots D_{n-c,j}^{m_j})$;
12 **Return:** L

4 Modular Algorithms

We use the results of Section 2 on the exact decomposition strategy presented in Section 3. We develop an algorithm which takes as input an ideal $\mathfrak{a}$ with generators in $\mathbb{Q}[\mathbf{X}]$, defining an equidimensional algebraic set $\mathscr{W}$ in $\mathbb{C}^n$ of dimension c, and gives as output the number of primary components, their degrees, multiplicities and the affine Hilbert function of the components of multiplicity 1.

Remark 4.1. *We did not present a non-modular version of Algorithm 4, since all the algorithms presented in Section 3.1 are not actually used. We insert this further procedure to avoid useless computations in the calling of Algorithm 5 in Step 9 of Algorithm 3.*

Algorithm 3: Modular Algorithm for affine Hilbert Function

Data: $\mathfrak{a} = (F_1, \ldots, F_m)$, $F_i \in \mathbb{Q}[X_1, \ldots, X_n]$, $\mathfrak{a}$ equidimensional with dimension c

Result: The degree and multiplicity of the primary components of $\mathfrak{a}$; for primary components of multiplicity 1, their initial ideal with respect to a degree compatible term ordering.

Preprocessing: Perform a generic integer change of coordinates on $\mathfrak{a}$, with coefficients in $\mathbb{Z}$;

Fix $(n-c)$ different coordinate linear spaces of dimension $c+1$, defined by set of indexes H_i, $i = 1, \ldots, n-c$;

Compute $D_1(0, \ldots, 0, X_{c+1})$ as the only generator of $GB_{elim(1)}(\mathfrak{a}|_{X_1=0,\ldots,X_c=0})$ respecting (3.6);

Compute the rational factorization: $D_1(0, \ldots, 0, X_{c+1}) = d_1^{(1)}(X_{c+1})^{m_1} \cdots d_s^{(1)}(X_{c+1})^{m_s}$;

for *j from 1 to s* **do**

  Choose a prime integer p_j dividing $d_j^{(1)}(0)$;

  Compute $D_i \mod p_j$ as the only polynomial in $GB_{elim(i)}(\mathfrak{a}) \mod p$ respecting (3.6), $i = 1, \ldots, n-c$;

  Compute the modular factorizations $D_i \mod p_j$, $i = 1, \ldots, n-c$;

  Apply Algorithm 4 to the rational factor $d_j^{(1)}(X_{c+1})$ and the modular factors of D_1, obtaining the set of modular factors $\mathcal{D}_j$ of D_1;

  Choose $D_{j\tilde{k}}^{(1)} \mod p_j \in \mathcal{D}_j$ of minimal degree such that $r_j = \frac{\deg d_j^{(1)}}{\deg D_{j\tilde{k}}^{(1)}} \in \mathbb{Z}$;

  if $r_j \geq 2$ **then**

    Apply Algorithm 5 to match the modular factor $D_{j\tilde{k}}^{(1)}$ with $D_{j\tilde{k}}^{(i)}$ modular factor of D_i, obtaining $\tilde{\mathfrak{a}}_i^{(j)} = \mathfrak{a} + \sum_{i=1}^{n-c}(D_{j\tilde{k}}^{(i)})^{m_j} \mod p_j$ (after re-labeling of the factors);

    if *m_j is 1* **then**

      Compute the Jacobian matrix of $\mathfrak{a} \mod p_j$ and a minor of size $(n-c) \times (n-c)$, $\widetilde{M}$;

      Compute $(\tilde{\mathfrak{a}}_i^{(j)} : \widetilde{M}) \mod p_j$;

    end

  end

end

Return: s number of rational components

for every $j = 1, \ldots, s$

r_j number of non-rational components constituting the rational component $\mathfrak{q}_j$

$\deg D_{j\tilde{k}}^{(1)}$ degree of each non-rational component of $\mathfrak{q}_j$

m_j multiplicity of the non-rational component

if $m_j = 1$, p_j and $(\tilde{\mathfrak{a}}_i^{(j)} : \widetilde{M}) \mod p_j$ ideal having the same initial ideal and same Hilbert function as $\mathfrak{q}_{1j}$

if $m_j \geq 2$, p and $D_{j\tilde{k}}^{(i)}$, $i = 1, \ldots, n-c$, image modulo p of $(n-c)$ a polynomial contained in $\mathfrak{q}_i^j$ but not in the other absolute components of $\mathfrak{a}$;

Algorithm 4: Partition of modular factors

Data: $d(X_{c+1}) \in \mathbb{Q}[X_{c+1}]$, an integer p dividing $d(0)$ and
$D(X_1, \ldots, X_{c+1}) = \prod_{i=1}^{l} D_i(X_1, \ldots, X_{c+1})^{m_i} \mod p$ such that
$d(X_{c+1}) \mid D(0, \ldots, 0, X_{c+1}) \mod p$

Result: A set containing the modular factors of $d(X_{c+1}) \mod p$

$A :=$ empty list, $i := 1$, $\delta := 1$;
while $i \leq l$ **do**
  $m_i :=$ multiplicity of $d(X_{c+1})$ in the rational factorization of $D(0, \ldots, 0, X_{c+1})$;
  if $D_i(0, \ldots, 0, X_{c+1}) \mod p$ *divides* $d(X_{c+1}) \mod p$ **then**
    add $D_i(X_1, \ldots, X_{c+1}) \mod p$ to A;
    $\delta = \delta \cdot D_i(0, \ldots, 0, X_{c+1}) \mod p$;
    if $\delta = d(X_{c+1}) \mod p$ **then**
      $i := l + 1$;
    end
  end
  $i := i + 1$;
end
Return: A

Algorithm 5: Matching of modular factors through affine Hilbert Dimension

Data: $D_i^{(1)}$ modular factor of $D_1(X_1, \ldots, X_{c+1})$ and $\{D_k^{(j)} \mod p\}_{\substack{j=2,\ldots,n-c \\ k=1,\ldots,m}}$ modular factors of D_j

Result: $\tilde{\mathfrak{a}}_i^j = \mathfrak{a} + \sum_{j=1}^{n-c} (D_i^{(j)})^{m_i} \mod p$ with Hilbert dimension c

Consider a $(n-c-1)$-uple $(D_k^{(j)})_{j=2,\ldots,n-c}$ such that $\deg(D_k^{(j)}) = \deg(D_i^{(1)})$ and $m_k = m_i$;
Compute $h =$Hilbert Dimension of $\mathfrak{a} + D_i^{(1)} + \sum_{j=2}^{n-c} (D_k^{(j)})^{m_k} \mod p$ with $(n-c)$ variables evaluated to 0;
if $h = 0$ **then**
  renumber the modular factor putting $D_i^{(j)} := D_k^{(j)}$
else
  go back to Step 1 and change $(n-c)$-uple.
end
Return: $\tilde{\mathfrak{a}}_i^j = \mathfrak{a} + (\sum_{j=1}^{n-c} D_i^{(j)})^{m_i} \mod p$.

4.1 Proof of Algorithm 3

We apply the results of Section 2 to the decomposition strategy explained in Section 3 and to the Algorithms of Section 3.1. Again, we deal with an equidimensional polynomial ideal $\mathfrak{a} = (F_1, \ldots, F_m)$ with dimension c, $F_i \in \mathbb{Q}[\mathbf{X}]$. The key point of Algorithm 3 is the choice of a prime integer p_i which gives a "modular image" of the algebraic number α_i s.t. $\mathfrak{q}_i^{(j)} \subseteq \mathbb{Q}(\alpha_i)[\mathbf{X}]$. For all the notations used, we refer to Section 3.1, Algorithms 3, 4 and 5.

We will now follow the steps of Algorithm 3 in order to show that it gives a correct output.

In Step 1 of Algorithm 3, as in Algorithm 1, we perform a generic change of coordinates; thanks to this, the projections on the "coordinate" linear spaces of dimension $c+1$ are "generic" in the sense of Proposition 3.2: the components of the projected algebraic set are in one-to-one correspondence with the components of the algebraic set itself (see also Corollary 3.3). Furthermore, consider on one hand the absolute factors of the polynomial whose zero set is the projected algebraic set and on the other one the primary components of the ideal defining the algebraic set: factors and primary components are in one-to-one correspondence and the degree and multiplicity of a factor is the degree and multiplicity of the corresponding primary component (in the sense of Definition 1.5 and 1.6).

In Step 2 we fix $(n-c)$ distinct "coordinate" linear spaces H_i (as explained in Section 3.1). Using projections on these linear spaces, we would like to apply the techniques for absolute factorization developed in [3], but we have to be careful because we do not have one of the main hypothesis: the Input of the Abs-Fact Algorithm presented in [3] is a *rationally irreducible* polynomial. This is not our case, this is why in Step 3 of the algorithm we compute a univariate factorization.
Indeed, assume that we are able to compute D_1, the only polynomial in the first $c+1$ variables of $GB_{elim(1)}(\mathfrak{a})$. This multivariate polynomial in general is not rationally irreducible; furthermore it is not advantageous to compute the multivariate rational factorization of D_1.
We rely on Hilbert's Irreducibility Theorem: for infinite integer specialization of c variables, a rationally irreducible factor of the polynomial D_1 stays rationally irreducible. This means that if

$$D_1(X_1, \ldots, X_{c+1}) = d_1^{(1)}(X_1, \ldots, X_{c+1})^{m_1} \cdots d_s^{(1)}(X_1, \ldots, X_{c+1})^{m_s} \in \mathbb{Q}[X_1, \ldots, X_{c+1}]$$

then for infinite $x_1, \ldots, x_c \in \mathbb{Z}$ the rational factorization of $D_1(x_1, \ldots, x_c, X_{c+1})$ is exactly

$$D_1(x_1, \ldots, x_c, X_{c+1}) = d_1^{(1)}(x_1, \ldots, x_c, X_{c+1})^{m_1} \cdots d_s^{(1)}(x_1, \ldots, x_c, X_{c+1})^{m_s} \in \mathbb{Q}[X_{c+1}].$$

Thanks to the generic change of coordinates of the Preprocessing Step, we can take $x_1 = \cdots = x_c = 0$. In order to compute this rational univariate factorization without computing $D_1(X_1, \ldots, X_{c+1})$, in Step 7 we simply specialize c variables of $F_1, \ldots, F_m$ and then compute the elimination Groebner Basis:

$$D_1(0, \ldots, 0, X_{c+1}) \in GB_{elim(1)}(\mathfrak{a}|_{X_1=0,\ldots,X_c=0}).$$

Since we are considering a generic projection, a rational factor of $D_1(X_1, \ldots, X_{c+1})$ corresponds to a rational component of the algebraic set $\mathscr{W} = V(\mathfrak{a})$ (in the sense of Definition 1.8), while each absolute factor of corresponds to an irreducible component.

Once computed in Step 4 the univariate rational factorization, we then proceed in order to "break" the non-rational components.
We consider the j-th factor of the rational factorization of D_1, that is $d_j^{(1)}(X_{c+1})$ which has multiplicity m_j. If the corresponding factor $d_j^{(1)}(X_1, \ldots, X_{c+1})$ of the univariate rational factorization of $D_1(X_1, \ldots, X_{c+1})$ is not absolutely irreducible, then its absolute factors have coefficients in some algebraic extension $\mathbb{Q}(\alpha_j)$. Using [3], Lemma 11, we can assume that the algebraic extension $\mathbb{Q}(\alpha_j)$ is generically generated by the evaluation of one absolute factor in a point with integer coordinates.

Thanks to the generic change of coordinates, we will choose $(0,\ldots,0) \in \mathbb{Z}^{c+1}$.
We choose an integer prime p_j dividing $d_j(0)$ (Step 6) applying Lemma 2.3 and, relying on randomness, we assume that the chosen prime p_j will preserve the initial ideal of the Groebner Basis we will compute along the "FOR" loop (as in Lemma 2.5). Thanks to Lemma 2.3, if we factor $D_1(X_1,\ldots,X_{c+1})$ modulo this prime p_j, the rationally irreducible factor $d_j^{(1)}(X_1,\ldots,X_{c+1})$ splits (if it is not absolutely irreducible). The homomorphism ψ_{p_j} of (2.2) is implicitly defined.
Actually we do not compute $D_1(X_1,\ldots,X_{c+1})$: in fact, in Step 7 we compute directly the modular elimination Groebner Basis and then the modular factorizations (Step 8). In Step 9 we group the modular factors corresponding to $d_j^{(1)}(X_{c+1})$ using Algorithm 4.

If the rational factor $d_j^{(1)}(X_1,\ldots,X_{c+1})$ is absolutely irreducible, then it does not further split modulo p_j, that is r_j, the number of modular factors of $d_j^{(1)}$, is exactly 1. In this case, we can stop here and repeat the loop for the next rational factor.
If $d_j^{(1)}(X_1,\ldots,X_{c+1})$ is absolutely reducible, then $r_j \geq 2$ (thanks to the choice of p_j according to Lemma 2.3): in Step 10 we choose a modular factor among them having minimal degree which divides $\deg d_j^{(1)}(X_{c+1})$; we assume that this factor is $D_{j\tilde{k}}^{(1)}(X_1,\ldots,X_{c+1})$.
In Step 12 we look for the corresponding modular factor of D_i, $i = 2,\ldots,n-c$. Using Algorithm 5, we obtain the ideal $\tilde{\mathfrak{a}}_{\tilde{k}}^j = \mathfrak{a} + \sum_{i=1}^{n-c}(D_{j\tilde{k}}^{(i)})^{m_j} \mod p_j$ with Hilbert dimension c. Corollary 2.7 certifies that $\tilde{\mathfrak{a}}_{\tilde{k}}^j = \psi_{p_j}(\mathfrak{a}_{\tilde{k}}^j)$.

Once defined in Step 12 the ideal $\tilde{\mathfrak{a}}_{\tilde{k}}^j$ (re-ordering the indexes) with affine Hilbert dimension c, if the multiplicity m_j is 1, we can keep on following Steps 5 and 8 of Algorithm 1: we compute the Jacobian Matrix of $\mathfrak{a} \mod p_j$ and consider one of its $(n-c)\times(n-c)$-minors, $\widetilde{M}$. We compute the colon ideal of $\tilde{\mathfrak{a}}_{\tilde{k}}^j$ with $\widetilde{M}$. Let M be the $(n-c)\times(n-c)$ minor of the Jacobian matrix of $\mathfrak{a}$ s.t. $M \mod p_j = \widetilde{M}$.

We need to show that for infinite primes p_j the colon ideal modulo p_j has the same affine Hilbert function of the colon ideal in $\mathbb{Q}(\alpha_j)[X_1,\ldots,X_n]$, that is $\psi_{p_j}(\mathfrak{a}_{\tilde{k}}^j : M) = (\tilde{\mathfrak{a}}_{\tilde{k}}^j : \widetilde{M})$.
First of all, observe that $\tilde{\mathfrak{a}}_{\tilde{k}}^j$ and the corresponding non-modular ideal $\mathfrak{a}_{\tilde{k}}^j$ have the same Hilbert function for all but a finite number of prime integers (thanks to Theorem 2.6).
Furthermore, we can assume that we compute Jacobian matrix of $\mathfrak{a}$ and a minor M and then reduce modulo p_j. For what concerns the colon ideal, the actual computation is performed using a Groebner Basis (see [7], Chapter 4, §4, Theorem 11 for the details). This means that again we can apply Lemma 2.5 and so there is only a finite number of primes p_j such that $\psi_{p_j}(\mathfrak{a}_{\tilde{k}}^j : M)$ and $(\tilde{\mathfrak{a}}_{\tilde{k}}^j : \widetilde{M})$ differ.

Remark 4.2. *Actually, Algorithm 3 is a Las-Vegas one, just like the Abs-Fact Algorithm of [3]: 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 $S \in \mathbb{Z}$.*

We shall then modify the Preprocessing Step of Algorithm 3 and insert a small loop in Step 10, in order to stop the execution and go back to the Preprocessing Step, if we cannot define a $r_j \in \mathbb{Z}$ (see Abs-Fact Algorithm of [3]).

We can also compute the "minimal " rational algebraic extension $\mathbb{L}_i = \mathbb{Q}(\alpha_i)$ containing a set of generators of the ideal $\mathfrak{a}_i$. We can apply the LLL method developed in [3]. Unluckily, we do not have a technique to estimate the needed level of accuracy. We can just try to compute the minimal polynomial which defines $\mathbb{L}_i$ with increasing levels of accuracy and stop when we get the same polynomial $q(T)$ with 2 different levels of accuracy.

5 Tricks on an example

The data and Maple files of the examples we are going to discuss are available at
https://sites.google.com/site/cristinabertone/examples-for-modular-decomposition

We now test our algorithm on a quite simple example (see the file *DecompositionCIcurveDegree48.mw*).

We consider a complete intersection ideal $\mathfrak{a} \subseteq \mathbb{C}[X,Y,Z]$ generated by two polynomials with rational coefficients, $F, G \in \mathbb{Q}[X,Y,Z]$, of degree 8 each, rationally irreducible.
We constructed this c.i. curve in such a way that we know that it has non trivial primary components, in particular it has a rational primary component of degree 14, that splits in 2 absolute primary components of degree 8 each, generated by polynomials in $\mathbb{Q}(\sqrt{2})[X,Y,Z]$.

The complete intersection curve $\mathcal{C} = V(\mathfrak{a})$ has degree 48 (one can see this, for instance, using a generic plane section and counting points with multiplicity).
Since $\mathfrak{a}$ is generated by 2 polynomials, we can use resultants instead of elimination Groebner Basis to compute the elimination of variables. 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 14 and multiplicity 1;
- $d_2^{(1)}(Y)$ factor of degree 4 and multiplicity 1;
- $d_3^{(1)}(Y)$ factor of degree 22 and multiplicity 1;
- $d_4^{(1)}(Y)$ factor of degree 2 and multiplicity 2;
- $d_5^{(1)}(Y)$ factor of degree 1 and multiplicity 4.

So, using Definition 1.8, the complete intersection $\mathfrak{a}$ has 5 rational components $\mathfrak{q}_i$, three of them with multiplicity 1, with degrees given by $\deg d_i^{(1)}(Y)$ (thanks to Corollary 3.3).

We can proceed in the following way: for each rational factor $d_i^{(1)}(Y)$, we choose a prime number p_i dividing $d_i^{(1)}(0)$, except for $i = 5$: indeed, we do not look for a prime dividing $d_5^{(1)}(0)$, since this rational component will not further split. We then compute the projections on the coordinate plane modulo p_i, $i = 1, \ldots, 4$. Then we compute the modular polynomial describing the projection of the curve for each prime p_i and its modular factorization. We know that p_i forces the rational factor corresponding to $d_i^{(1)}(Y)$ to split (if it is absolutely reducible). We check whether there is a prime p_j between the chosen ones such that it forces all of the rational factors: if we find one, we can perform all of the computations modulo this prime. If not, we can in any case choose to compute modulo "some" of the primes p_i: if p_i and p_j both give the desired splitting for the i-th and j-th rational factor, then we can compute the corresponding ideals modulo p_i (and not use p_j).

For the ideal $\mathfrak{a}$, we see that $p = 89$ give the desired splitting for all of the 4 rational factors which may be absolute reducible. So we will compute only modulo 89.

The computations of $D_1(X,Z) = Res_Y(F,G) \mod p$, $D_2(X,Y) = Res_Z(F,G) \mod p$ and their modular factorization take less than 4 seconds each.

All of the rational factors further split modulo p in 2 factors. So we compute the initial ideal (and affine Hilbert function) for one of the two absolute components of degrees 7, 2 and 11. The

other absolute components have multiplicity > 1, so we do not perform on them Steps 14 and 15 of Algorithm 3.

Performing Algorithm 3 (including the matching of the factors through Algorithm 5), we then obtain the initial ideals:

- $\deg q_1^{(1)} = 7$, $in_{tlex}(\mathfrak{q}_1^{(1)}) = (X^3, Y^7, X^2Z^2, X^2Y, XY^3, XZ^5XY^2Z^2XYZ^3)$;
- $\deg q_2^{(1)} = 2$, $in_{tlex}(\mathfrak{q}_2^{(1)}) = (X, Y^2)$;
- $\deg q_3^{(1)} = 11$, $in_{tlex}(\mathfrak{q}_3^{(1)}) =$
  $= (X^3, Y^{11}, XZ^9, X^2Y^2, XY^2, X^2Z^3, XY^4Z, X^2YZ^2, XY^3Z^3, XY^2Z^5, XYZ^7)$.

Finally, we use the techniques of the Abs-Fact Algorithm of [3] to compute the polynomial $q(T) \in \mathbb{Z}[T]$ which defines the algebraic extension containing the coefficients of a set of generators for the absolute primary components. However we do not have an a priori bound on the size of the coefficients of $q(T)$, as pointed out in Remark 4.2). We perform an Hensel Lifting of a modular univariate factor until a quite high level of accuracy (in this case, until p^{512}); we then construct different candidates for the minimal polynomial, starting with accuracy p^{16}, until two different levels of accuracy give the same polynomial.

For accuracy p^{64}, we see that the minimal polynomial "stabilizes":

$$q(T) = 26301054375\,T^2 - 214355874045600\,T + +436754388124393216$$

Obviously, since $\deg q(T) = 2$, we can easily find a better presentation of the extension $\mathbb{Q}(\alpha)$ computing the roots of $q(T)$: 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

$$\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \mathfrak{q}_3 \cap \mathfrak{q}_4 \cap \mathfrak{q}_5$$

with $\deg \mathfrak{q}_1 = 14$, $\deg \mathfrak{q}_2 = 4$, $\deg \mathfrak{q}_3 = 22$, $\deg \mathfrak{q}_4 = 2$ and $\deg \mathfrak{q}_5 = 1$ and multiplicities $m_1 = m_2 = m_3 = 1$, $m_4 = 2$, $m_5 = 4$.

Each of the rational primary ideals with multiplicity 1 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 $\sigma(\sqrt{2}) = -\sqrt{2}$.

The whole computation took less than 15 minutes on a home-use personal computer, without any problem with memory allocation.

We point out that it is not that obvious to obtain this kind of information about the decomposition of the ideal $\mathfrak{a}$. For instance, one may use one of the most popular Computer Algebra System, Maple [18].

We tried to use the Maple command `PrimaryDecomposition` (whose algorithm is based on [13]), which gives as an output the primary decomposition of the ideal $\mathfrak{a}$. As input, we also gave the algebraic extension of the rationals in which one can find the generators of the absolute primary decomposition of $\mathfrak{a}$, namely $\mathbb{Q}(\sqrt{2})$. Even with this further information about the decomposition (which is not a priori known from the only knowledge of the rational generators of $\mathfrak{a}$), `PrimaryDecomposition` in Maple caused a problem with memory allocation (reaching about 2.3 GB), after computing for more than 1 hour.

For what concerns other computer algebra systems, we also tried Singular ([14]), 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 [13], the algorithms are described in [9]). In both cases we stopped the computations after 2 hours, without obtaining the primary decomposition.
The CAS CoCoA([6]) has a command `PrimaryDecomposition` to decompose only monomial square-free ideals. It also has a command called `EquiIsoDec` which computes an equidimensional isoradical decomposition of $\mathfrak{a}$, i.e. a list of equidimensional ideals $\mathfrak{b}_1, \ldots, \mathfrak{b}_k$ such that the radical of $\mathfrak{a}$ is the intersection of the radicals of $\mathfrak{b}_1, \ldots, \mathfrak{b}_k$. This command is based on the algorithm presented in [4] and it works only using $\mathbb{Q}$ or finite fields as coefficient ring. Nevertheless, `EquiIsoDec` could not give the output on our example after more than two hours computing.

Although for the moment we cannot really compare our algorithm with the above ones mentioned, we can see that the problem we are facing is challenging and that our modular strategy may move around the computational problems of primary decomposition. Nevertheless, we cannot give complete comparaison for the moment, since we cannot compute the complete primary decomposition nor a reduced decomposition: using Algorithm 3 we get several interesting data about the absolute primary components of an equidimensional ideal. Indeed, these data may be useful as a guide or a bound for numerical algorithms, such as the ones in [12] or [21].

Furthermore, the technique taken from [3] to construct the algebraic extension containing the coefficients of a set of generators of a primary component, could be used with other algorithms: for instance, one can see the example *DecompositionCIcurveDegree36.mw*. With our modular strategy, we obtain not only the initial ideal of all of the absolute primary components of a complete intersection in $\mathbb{Q}[X,Y,Z]$ generated by 2 polynomials both of degree 6, but also that $\mathbb{Q}(\sqrt{2})$ contains the coefficients of the generators of these components.
If we ask Maple to compute the primary decomposition of this ideal, again it does not reach the result after one hour of computation. But if we pass to the command `PrimaryDecomposition` also the information that the primary components are inside $\mathbb{Q}(\sqrt{2})[X,Y,Z]$, then we obtain the primary decomposition in less than 3 minutes.

This example suggests that we may combine at least a part of our strategy (for instance, the construction of the "splitting" field) with an existing algorithm (such as the one implemented in Maple), in order to obtain a complete result.

Conclusions and future work

In this paper we designed an algorithm which, given a set of polynomials with rational coefficients defining an equidimensional ideal $\mathfrak{a}$, returns the initial ideal of each absolute prime component of $\mathfrak{a}$. Furthermore it also returns information concerning non-reduced primary components, such as their number, degree, multiplicity. The main ingredients of the algorithm are the classical technique of projection and the use of computations modulo well-chosen primes, as done in [3] in order to decompose a bivariate polynomial. The obtained results seem promising, mostly for what concerns complete intersections and more precisely, for curves in $\mathbb{C}^3$.

A further step is to implement this algorithm in a Computer algebra System, for instance in Mathemagix [19]. Mathemagix is a free computer algebra system under development, which has available libraries for algebraic computation (such as large numbers, polynomials and others) for exact and approximate computation. This should make Mathemagix particularly suitable as a bridge between symbolic computation and numerical analysis.

Our final aim is actually to design an algorithm which uses projections with modular techniques and can return the complete absolute primary decomposition of the ideal given as input. The main obstacle to this is the absence of a tool similar to Hensel's Lifting (see for instance [23], Chapter 15,

Section 4), which allows lifting a modular factorization to a rational one; we would need a generalization of this in order to lift the modular decomposition of an ideal.

Our next task is then to develop such a tool, design and implement a primary decomposition algorithm and compare its efficiency with other implemented routines. With this tool, we may be able to obtain a complete decomposition for the reduced part of an equidimensional ideal.

Other possible improvements of the algorithm are dealing with a non-equidimensional ideal $\mathfrak{a}$ and computing also non-reduced primary components; for the first part we will have to choose whether dealing only with the top-dimensional part of $\mathfrak{a}$ or studying also smaller components; for the second one, if we will be able to compute these non-reduced primary components, then we will also be able to compute a radical decomposition (see [4]).

We are hopeful that our techniques are competitive, since at this moment we can already get a lot of information concerning the absolute decomposition of an ideal, in a reasonable time with a limited use of memory, while other CAS cannot really deal with the primary decomposition of the same ideal (see Section 5). So, even if at the moment the results of our method are partial and cannot be directly compared to the performances of other softwares, we believe that this method is on the right path to get an efficient primary decomposition algorithm.

Acknowledgements

The author is grateful to her Ph.D. advisors Andre Galligo and Margherita Roggero for their constant support and encouragement. The author also wish to thank Gregoire Lecerf for valuable discussions about the subject and the research group Galaad (Inria Sophia Antipolis, France) where she worked during her Ph.D. thesis.

References

[1] 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.

[2] Dan Bates, Chris Peterson, and Andrew J. Sommese. A numerical-symbolic algorithm for computing the multiplicity of a component of an algebraic set. *Journal of Complexity*, 22(4):475 – 489, 2006.

[3] 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.

[4] Massimo Caboara, Pasqualina Conti, and Carlo Traverso. Yet another ideal decomposition algorithm. Mora, Teo (ed.) et al., Applied algebra, algebraic algorithms and error-correcting codes. 12th international symposium, AAECC-12, Toulouse, France, June 23–27, 1997. Proceedings. Berlin: Springer. Lect. Notes Comput. Sci. 1255, 39-54 (1997)., 1997.

[5] 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.

[6] CoCoATeam. CoCoA: a system for doing Computations in Commutative Algebra. Available at http://cocoa.dima.unige.it, 2009.

[7] 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.

[8] 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.

[9] 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.

[10] Clémence Durvye. Evaluation techniques for zero-dimensional primary decomposition. *J. Symb. Comput.*, 44(9):1089–1113, 2009.

[11] David Eisenbud. *Commutative algebra. With a view toward algebraic geometry.* Graduate Texts in Mathematics. 150. Berlin: Springer-Verlag. , 1995.

[12] André Galligo and David Rupprecht. Irreducible decomposition of curves. *J. Symb. Comput.*, 33(5):661–677, 2002.

[13] Patrizia Gianni, Barry Trager, and Gail Zacharias. Gröbner bases and primary decomposition of polynomial ideals. *J. Symb. Comput.*, 6(2-3):149–167, 1988.

[14] 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.

[15] Robin Hartshorne. *Algebraic geometry. Corr. 3rd printing.* Graduate Texts in Mathematics, 52. New York-Heidelberg-Berlin: Springer- Verlag. XVI, 1983.

[16] Grete Hermann. Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. *Math. Ann.*, 95(1):736–788, 1926.

[17] Martin Kreuzer and Lorenzo Robbiano. *Computational commutative algebra. II.* Berlin: Springer. x, 586 p., 2005.

[18] Maplesoft. Maple - Math and Engeneering Software. see `http://www.maplesoft.com/`, 2009.

[19] Mathemagix. A free computer algebra system. Available at `http://www.mathemagix.org`, 2009.

[20] A. Seidenberg. Constructions in algebra. *Trans. Amer. Math. Soc.*, 197:273–313, 1974.

[21] 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.

[22] Peter Stevenhagen and Hendrik W.jun Lenstra. Chebotarëv and his density theorem. *Math. Intell.*, 18(2):26–37, 1996.

[23] Joachim von zur Gathen and Jürgen Gerhard. *Modern computer algebra. 2nd ed.* Cambridge University Press, 2003.