Algorithms for Primary Decomposition

Since 1864

Name : Nazeran Idrees

Year of Admission : 2006

Registration No. : 78-GCU-PHD-SMS-06

Abdus Salam School of Mathematical Sciences

GC University Lahore, Pakistan.

Algorithms for Primary Decomposition

Submitted to

Abdus Salam School of Mathematical Sciences

GC University Lahore, Pakistan

In the partial fulfillment of the requirements for the award of degree of

Doctor of Philosophy

in

Mathematics

By

Name : Nazeran Idrees

Year of Admission : 2006

Registration No. : 78-GCU-PHD-SMS-06

Abdus Salam School of Mathematical Sciences

GC University Lahore, Pakistan.

DECLARATION

I, **Nazeran Idrees** Registration No. **78-GCU-Ph.D-SMS-06** student at **Abdus Salam School of Mathematical Sciences GC University** in the subject of **Mathematics** admitted in **2006**, hereby declare that the matter printed in this thesis titled

"Algorithms for Primary Decomposition"

is my own work and that

(i) I am not registered for the similar degree elsewhere contemporaneously.

(ii) No direct major work had already been done by me or anybody else on this topic; I worked on, for the Ph. D. degree.

(iii) The work, I am submitting for the Ph. D. degree has not already been submitted elsewhere and shall not be submitted in future by me for obtaining similar degree from any other institution.

Dated: ---------- ----------

Signature

RESEARCH COMPLETION CERTIFICATE

Certified that the research work contained in this thesis titled

"Algorithms for Primary Decomposition"

has been carried out and completed by **Ms. Nazeran Idrees** Registration No. **78-GCU-Ph.D-SMS-06** under my supervision.

---------- ----------

Date Supervisor

Gerhard Pfister

Submitted Through

Prof. Dr. A. D. Raza Choudary ----------

Director General Controller of Examination

Abdus Salam School of Mathematical Sciences GC University, Lahore

GC University, Lahore, Pakistan.

To my Mother and Daughter

Table of Contents

Abstract

The primary decomposition methods of Eisenbud, Huneke and Vasconcelos are analysed in detail providing proofs of important theorems and all the corresponding algorithms are programmed in the language of SINGULAR. MOreover, we investigated the parallelization of two modular algorithms. In fact, we consider the modular computation of Gröbner bases (resp. standard bases) and the modular computation of the associated primes of a zero–dimensional ideal and describe their parallel implementation in SINGULAR. The algorithms of Shimoyama and Yokoyama for primary decomposition of ideals are generalized to submodules of a free module over the polynomial ring in several variables with coefficients in a field. The algorithms are implemented in SINGULAR.

Acknowledgements

Thanks GOD!
I would like to say a very special and warm "Thank You" to Dr. Gerhard Pfister, my supervisor, for his wonderful suggestions and constant support during this research. I am also thankful to Dr. A D Raza Choudhary for providing me with best research facilities and challenging environment.

A very hearty thanks goes to my mother who is also my first teacher of mathematics, for all her love,guidance and constant encouragement throughout my learning . I am much grateful to all my teachers; especially to Barbu Berceanu, Herzog, Popescu, Tiberieu, Vakhtan Lomadze for all their help and guidance.

This research wouldn't have been possible without using SINGULAR. I should also mention that my PhD studies is supported in part by GC University Faisalabad, Government of Punjab and The Higher Education Commission of Pakistan. I would like to thank all the administrative staff of ASSMS who supported me directly or indirectly.

The most heavy cost during my PhD is paid by my darling daughter Maryam who have to miss many motherly cares, for which I am indebted for my whole life. Nusrat, Yasir and Saima are friends of my hard times during my research, I am thankful to them for all their love, support and cooperation. I owe thanks to my friend Afshan for her friendship and for all the wonderful moments we spent together. Words cant express thanks to my husband for all his love, devotion and patience. I also owe thanks to my parents in law as well as my sisters and brother in law for all their support and kindness.

Lahore, Pakistan — Nazeran Idrees
October 27, 2010

Introduction

The primary decomposition of ideals is a fundamental tool in commutative algebra . Algebraically it generalizes the concept of factorization to intersection of irreducible ideals. Geometrically the primary decomposition of radical ideals corresponds to the decomposition of an affine variety into irreducible varieties. The efficient and fast computation of primary decomposition of ideals in a polynomial ring and modules over polynomial rings has been one of the most challenging tasks in Computer Algebra since many years.

Many different algorithms have been developed over time for the computations of primary decomposition. Mainly there are three different approaches to compute the primary decomposition; One of them is developed by Gianni, Trager and Zacharias(cf. [GTZ88]) which exploits the structure of Gröbner basis and reducing an ideal to zero-dimensional by generic linear coordinate change. In Chapter 1 basic concepts of primary decomposition of a submodule U of a finitely generated Ω–module V, where $\Omega = \mathbb{F}[\xi_1, \ldots, \xi_n]$ is a ring of polynomials over field $\mathbb{F}$, is discussed. The uniqueness theorems and the existence of primary decompositions as well as the method of Gianni, Trager and Zacharias(cf. [GTZ88]) for primary decomposition of ideals and modules is recalled in this chapter, which will be used further in finding the associated primes in second and third capter.

Another important technique of primary decomposition is introduced by Eisenbud, Huneke and Vasconcelos which is based on homological methods to reduce the problem of primary decomposition to equidimensional ideals. They characterise the intersection of primary modules of a module U of maximal dimension as the kernel of the canonical map $U \to \mathrm{Ext}^c_\Omega(\mathrm{Ext}^c_\Omega(U,\Omega),\Omega)$, c the codimension of U. The third section fills in many gaps of the paper of Eisenbud(cf. [EHV92]) by providing proofs of important theorems which include Theorem 1.3.5, Theorem 1.3.6 and Theorem 1.3.8. All corresponding algorithms in this section are programmed in SINGULAR which are included in the appendix.

The second chapter is about the parallelisation of two modular algorithms(cf. [IPS10]). We consider the modular computation of Gröbner basis and the modular computation of the associated primes of a zero dimensional ideal which uses the technique of lifting via chinese remainder theorem and Farey rational map, and describe their parallel implementation in SINGULAR. This technique remarkably speeds up the computation and it is tested for many examples. All the corresponding procedures are loades in the library "assprimeszerodim.lib".

The third approach towards primary decomposition is due to Shimoyama and Yokoyama(cf. [SY96]) which also relies on the computation of Gröbner basis, separating sets and decomposition of ideal into pseudo primary ideals. The third chapter deals with the generalisation of this method to submodules of modules in R^m with some examples.The corresponding algorithms are implemented in SINGULAR(cf. [Id09]).

Chapter 1

Mathematical Background

,

1.1 Primary Modules and Primary Decomposition

Let $\Omega = \mathbb{Q}[X]$, $X = \{\xi_1, \xi_2, \ldots, \xi_n\}$, be the polynomial ring over the the field of rational numbers $\mathbb{Q}$ and $U \subseteq \Omega^s$ be a submodule over Ω.
We use definitions, notations and basic results of cf. [E95] and [GP07], and recall some of them.

Definition 1.1.1. A prime ideal $\wp$ of Ω is said to be *associated* to Ω if $\wp$ is annihilator of some element of U i.e. $\wp = \{r \in \Omega \mid r\xi = 0; \xi \in U\}$.
The set of all primes associated to U is denoted by $\operatorname{Ass} U$.

From the definition we see that $\wp$ is an associated prime of U if and only if $\Omega/\wp$ is isomorphic to a submodule of U. Moreover, we can see that all the associated primes of U contain the annihilator of U. If an Ω-module U is the union of a family of submodules $(U_i)_{i\in I}$, then clearly

$$\operatorname{Ass} U = \cup_{i \in I} \operatorname{Ass} U_i$$

Definition 1.1.2. Let $\wp, \wp' \in \operatorname{Ass} U$ and $\wp' \subseteq \wp$, then $\wp$ is called *embedded* prime ideal of U. We define $\operatorname{Ass}(U, \wp) := \{\wp' \mid \wp' \in Ass(U), \wp' \subset \wp\}$.

Proposition 1.1.1. *Let U be a nonzero Ω-module and l be an ideal of Ω, which is maximal element of the set containing the annihilators of elements of U, then l is prime. In particular, if Ω is noetherian then $\operatorname{Ass} U$ is nonempty.*

Lemma 1.1.2. *If we have a short exact sequence of Ω-modules $0 \to U' \to U \to U'' \to 0$, then $\operatorname{Ass} U' \subset \operatorname{Ass} U \subset \operatorname{Ass} U' \cup \operatorname{Ass} U''$.*

Proposition 1.1.3. *Let Ω be a noetherian ring and U be a finitely generated Ω module, then there exists a filtration of U*

$$0 = U_0 \subset U_1 \subset \ldots \subset U_n = U$$

such that for some prime ideal $\wp_i$ $U_{i+1}/U_i \cong \Omega/\wp_i$.

Theorem 1.1.4. *Let Ω be a noetherian ring and U be a finitely generated Ω module. $\operatorname{Ass} U$ is a finite nonempty set of primes each containing $\operatorname{Ann} U$. The set $\operatorname{Ass} U$ contains all the prime ideals minimal among primes containing $\operatorname{Ann} U$.*

Theorem 1.1.5. *The union of associated primes of U consists of zero and the set of zero divisors of U.*

Theorem 1.1.6. *The localization at an arbitrary multiplicatively closed set Γ commutes with the formation of the set $\operatorname{Ass} U$, i.e*
$\operatorname{Ass}_{\Omega[\Gamma^{-1}]} U\Gamma^{-1} = \{\wp\Omega\Gamma^{-1} \mid \wp \in \operatorname{Ass} U \text{ and } \wp \cap \Gamma = \emptyset\}$

Definition 1.1.3. Let $U \subset V$ be submodules of free module $\Omega^s = \mathbb{F}[X]^s$. We say that U is a *primary submodule* of V if whenever $rv \in U$, for some $r \in \Omega, v \in U$, implies that either $v \in U$ or $r \in \sqrt{\text{Ann}\, V/U}$. Moreover, $\text{Ann}(V/U)$ is a primary ideal of Ω, and we say that U is $\sqrt{\text{Ann}(V/U)}$–primary in V.

Remark 1.1.1. Let $U \subset V$ be submodules of Ω^s and $\wp$ be a maximal ideal of Ω then U is $\wp$–primary submodule of V if and only if $\text{Ann}(V/U)$ is a $\wp$–primary ideal in Ω.

Definition 1.1.4. A submodule U of an Ω-module $V \subset \Omega^s$ has a *primary decomposition* if $U = \cap_{i=1}^{r} \Theta_i$ where each Θ_i is a $\wp_i$-primary submodule of V for some prime ideal $\wp_i$ of Ω. Θ_i is called the *primary component* of U associated to $\wp_i$ and each $\wp_i$ is an *associated prime* of U. If Θ_i does not contain $\cap_{j \neq i} \Theta_j$ and the $\wp_i$'s are all distinct then the decomposition is said to be *irredundant*. As intersection of a finite number of $\wp$-primary submodules of V is also $\wp$-primary, so *irredundant* primary decomposition of a module can always be deduced from any given primary decomposition. If $\wp_i$ is a minimal prime ideal among the set of all associated primes of U, then $\wp_i$ is called *isolated* prime associated to U; otherwise $\wp_i$ is *embedded*. The set of all minimal associated primes of U is called $\text{minAss}(U)$.

The Lasker-Noether decomposition theorem guarantees the existence of the primary decomposition.
For this we define irreducible modules:

Definition 1.1.5. Let U be a submodule of V then U is called *irreducible* submodule if it cannot be expressed as an intersection of two strictly larger submodules of V.

Theorem 1.1.7. *Every submodule $U \subset V$ can be expressed as a finite intersection of irreducible submodules of V.*

Theorem 1.1.8. *Every irreducible submodule $U \subset V$ is primary.*

From above two theorems we have the following conclusion:

Theorem 1.1.9. *Every submodule $U \subseteq \Omega^s$, where Ω is a noetherian ring with identity, has an irredundant primary decomposition.*

Remark 1.1.2. Let $U = \Theta_1 \cap \Theta_2 \cap \ldots \cap \Theta_r$ and $U = T_1 \cap T_2 \cap \ldots \cap T_s$ be two irredundant primary decompositions for U with each Θ_i a $\wp_i$-primary submodule of V and each T_j a $\wp'_j$-primary submodule of V then the number of primary components in both decompositions is same,i.e. $r = s$ and, $\wp_i = \wp'_i$, after some suitable reordering. Moreover, if $\wp_i$ is minimal then (with the same reordering) $\Theta_i = \Theta'_i$.
It can be readily observed that $\cap \operatorname{Ann}(V/\Theta_i)$ is a (not necessarily irredundant) primary decomposition for $\operatorname{Ann}(V/U)$.

Definition 1.1.6. Let $U \subseteq V$ be Ω-modules and $l \subseteq \Omega$ be an ideal. We define

i: the quotient of U by l in V as
$U :_V l := \{m \in V \mid l.m \subseteq U\}$,

ii: and the stable quotient of U by l in V as
$U :_V l^\infty := \{m \in V \mid \exists t > 0, l^t.m \subseteq U\}$.

Lemma 1.1.10. *Let U be a $\wp$–primary submodule of V. Then:*

1. $U :_V \xi = U$ *if* $\xi \notin \wp$.

2. $U :_V h = V$ *if* $h \in \Theta = \operatorname{Ann} V/U$.

Lemma 1.1.11. *Let Ω be a noetherian ring and $\Theta \subset V$ be a $\wp$–primary module over Ω.*

1. *The radical of* $\mathrm{Ann}(V/\Theta)$ *is a prime ideal.*

2. *Let T be a $\wp$–primary module, then $\Theta \cap T$ is also a $\wp$ primary module.*

3. *Let $r \in \Omega$ and $r \notin \mathrm{Ann}\, V/\Theta$ then $\Theta : r$ is $\wp$–primary. If $r \in \wp$ then $\Theta \subsetneq \Theta : (r)$.*

The First uniqueness theorem of primary decomposition is stated as:

Theorem 1.1.12. *Let $U = \Theta_1 \cap \Theta_2 \ldots \Theta_m$ be a minimal primary decomposition, where each Θ_i is $\wp_i$–primary submodule. Then $\wp_i$'s are precisely that prime ideals which occur in set* $\mathrm{Ass}(V/U)$ *and hence are independent of any particular decomposition of U.*

Proposition 1.1.13. *Let Γ be a multiplicatively closed subset of Ω and let U be a $\wp$–primary submodule of V.*

i. If $\Gamma \cap \wp \neq \emptyset$, then $\Gamma^{-1}\Theta = \Gamma^{-1}\Omega$.

ii. If $\Gamma \cap \wp = \emptyset$, then $\Gamma^{-1}\Theta$ is $\Gamma^{-1}\wp$–primary and its contraction in Ω is Θ.

Its proof is a straightforward generalization of corresponding theorem for ideals in cf. [AM69].

Corollary 1.1.14. *Let Ω be a noetherian ring and Γ be a mutiplicatively closed subset of Ω and let $U = \cap U_i$ be a minimal primary decomposition, and $\wp_i$ be the corresponding associated primes of U. Then*

$$\Gamma^{-1}U = \bigcap_{\wp_i \cap \Gamma = \emptyset} \Gamma^{-1}U_i, \quad \Gamma^{-1}U \cap V = \bigcap_{\wp_i \cap \Gamma = \emptyset} U_i$$

and these are also minimal decompositions

So we have the following conclusion:

Theorem 1.1.15. *The isolated primary components of U (i.e primary components of U corresponding to minimal associated primes) are uniquely determined.*

1.2 Primary decomposition using the method of Gianni, Trager and Zacharias

The minimal associated primes of ideals and modules in chapter 2 and 3, respectively, are computed using the method of Gianni, Trager and Zacharias (cf. [GTZ88]). So we give here a detailed description of the algorithm.
The zero dimensional ideals and modules are important in the sense that they have only maximal associated primes and we can reduce the primary decompositon of higher dimensional ideals and modules to zero dimensional case.

Definition 1.2.1. Let Ω be a ring. Let l be an ideal of Ω and V be an Ω module then dimension of the module V is $\dim V := \dim(\Omega/\operatorname{Ann} V)$.

Definition 1.2.2. Let l be an ideal of $\Omega = \mathbb{Q}[\xi]$. A subset $\xi' \subseteq \xi$ is said to be an *independent set relative to* l if $l \cap \mathbb{Q}[\xi'] = \{0\}$. An independent set ξ' relative to l is said to be *maximally independent* set relative to l if $l \cap \mathbb{Q}[\xi' \cup \{y\}] \neq \{0\}$, for every variable y in $\xi \setminus \xi'$
In general a subset $\xi' \subset \xi$ is independent with respect to a module $U \subseteq V$ if it is independent relative to the ideal $\operatorname{Ann} V/U$.

Remark 1.2.1. We will denote the lexicographical ordering of monomials in $\mathbb{F}[\xi_1, \ldots, \xi_n]$, with $\xi 1 > \ldots > \xi_n$, with ℓp.

Definition 1.2.3. Let $\Omega = \mathbb{F}[\xi_1, \xi_2, \ldots, \xi_n]$. A maximal ideal $l \subseteq \Omega$ is said to be in *normal position* with respect to ordering ℓp if there exist polynomials $h_1, h_2, \ldots, h_n \in \mathbb{F}[\xi_n]$ with $l = \langle \xi_1 + h_1(\xi_n), \ldots, \xi_{n-1} + h_{n-1}(\xi_n), h_n(\xi_n) \rangle$.

A zero dimensional ideal l is said to be in *normal position* with ordering ℓp, if all the associated primes $\{\wp_1, \ldots, \wp_s\}$ of l are in normal position and if $\wp_i \cap \mathbb{F}[\xi_n] \neq \wp_j \cap \mathbb{F}[\xi_n]$ for $i \neq j$.

A zero dimensional module $U \subseteq V$ is in *normal position* if $\mathrm{Ann}(V/U)$ is in normal position.

Proposition 1.2.1. *Let $\mathbb{F}$ be a field of characteristic zero, and let $l \subseteq \mathbb{F}[\xi]$, $\xi = \{\xi_1, \xi_2, \ldots, \xi_n\}$, be a zero dimensional ideal. Then there exists a zariski non–empty open set $\mathcal{O} \subset \mathbb{F}^{n-1}$ such that for all $\underline{u} = (u_1, u_2, \ldots, u_{n-1}) \in \mathcal{O}$, after the coordinate change $\phi_{\underline{u}} : \mathbb{F}[\xi] \longrightarrow \mathbb{F}[\xi]$ defined as $\phi_{\underline{u}}(\xi_i) = \xi_i$ if $i < n$ and*

$$\phi_{\underline{u}}(\xi_n) = \xi_n + \sum_{i=1}^{n-1} u_i \xi_i$$

$\phi_{\underline{u}}(l)$ is in normal position with respect to ℓp ordering.

Lemma 1.2.2. *Let U be a submodule of V with dimension zero and let $U = \cap U_i$ and $\mathrm{Ann}\, V/U = \cap \Theta_i$ be the irredundant primary decompositions, where Θ_i(respectively the U_i) are the $\wp_i$ primary components, then $\Theta_i = \mathrm{Ann}\, V/U_i$.*

Corollary 1.2.3. *Let U be a zero–dimensional submodule of V. Then U is $\wp$–primary if and only if $\mathrm{Ann}\, V/U$ is $\wp$–primary.*

Proposition 1.2.4. *Let $U \subseteq \mathbb{F}[\xi_1, \xi_2 \ldots \xi_n]^s$ be a zero dimensional module and let $\langle h \rangle = \mathrm{Ann}\, V/U \cap \mathbb{F}[\xi_n]$, $h = h_1^{\nu 1} h_2^{\nu 2} \ldots h_s^{\nu s}$ h_i monic and prime and $h_i \neq h_j$ for $i \neq j$, and let $g_i := \prod_{i \neq j} h_j^{\nu_j}$ then*

1. $U = \cap_{i=1}^{s} \langle U : g_i \rangle$.

2. *If* $l := \operatorname{Ann} V/U$ *is in normal position with ordering* ℓp*, then* $\langle l, h_i^{\nu_i} \rangle$ *is primary ideal for all* i.

This Proposition shows how to compute the primary decomposition of a zero dimensional module U in normal position by using the factorisation of g. In the algorithm of Gianni,Trager, Zacharias the module U is put in normal position by the map $\phi_{\underline{u}}$, $\underline{u} \in \mathbb{F}^{n-1}$ is choosen randomly. But, in practice, it is not sure that for a random selection of $\underline{u}$ made by computer, $\phi_{\underline{u}}(l)$ is in normal position. The following algorithm can be used as a criterion to test a zero dimensional ideal if it is primary and in normal position.

Algorithm 1.2.5. ***PrimalityTest(*** l ***)***

Input: *an ideal* $l \subset \mathbb{F}[\xi], \xi = (\xi_1, \xi_2 \ldots, \xi_n)$*, which is zero dimensional.*

Output: *if* l *is either not primary or not in normal position returns* $\langle 0 \rangle$*, otherwise* $\sqrt{l}$ *if the test is positive.*

- *find a reduced Gröbner basis of* l *with* ℓp *ordering;*
- *choose an element, say* $h \in S$*, with smallest leading monomial and factorise it;*
- *If* ($h = h_n^{\nu_n}$ *with* h_n *irreducible)*

  prm:=h_n*;*

  else

  return $\langle 0 \rangle$
- $j := n$*;*

- *While* $(j > 1)$

  $j := j - 1$*;*

  choose $g \in S$ *with* $lm(g) = \xi_j^m$*;*

  β*:=coefficient of* ξ^{m-1} *in* g *taken as a polynomial in* ξ*;*

  $t := \xi_j + \beta/m$*;*

  If $(t^m \equiv g \ mod \ prm)$

  prm:=prm+$\langle t \rangle$*:*

  else

  return $\langle 0 \rangle$*:*

- *return prm.*

Now the main steps to compute the primary decomposition of a zero dimensional module are given in the algorithm below:

Algorithm 1.2.6. ***ZeroDecGTZ(****U****)***

Input: *a zero dimensional module* $U \subset V$*.*

Output: *a set of pairs* $(\Theta_i, \wp_i)$ *where* Θ_i *is* $\wp_i$*–primary module and* $U = \cap_i \Theta_i$ *is a primary decomposition.*

- $res = \emptyset$, $l := \operatorname{Ann} V/U$*;*

- *select* $\underline{u} \in \mathbb{F}^{n-1}$ *randomly, and perform the coordinate change* $l' := \phi_{\underline{u}}(l)$, $U' := \phi_{\underline{u}}(U)$, $V' := \phi_{\underline{u}}(V)$*;*

- *compute a Gröbner basis* S *of* l' *with ordering* ℓp *and take an element* $h \in S$ *with smallest leading monomial.*

- *factorize* $h = h_1^{\nu 1} h_2^{\nu 2} \dots h_s^{\nu s} \in \mathbb{F}[\xi_n]$;

- *for* $j = 1$ *to* s *do*

  compute $g_j := \prod_{j \neq i} h_i^{\nu_i}$

  set $\Theta'_j := \langle l', h_j^{\nu_j} \rangle$ *and* $\Theta_j = \langle l, \phi_{\underline{u}}^{-1}(h_j^{\nu_j}) \rangle$;

  set $\wp'_j := PrimalityTest(\Theta'_i)$;

  If $\wp'_j \neq 0$

  set $\wp_j := \phi_{\underline{u}}^{-1}(\wp'_j)$, $U_i := (U : \phi_{\underline{u}}^{-1}(g_j))$;

  $res := res \cup (U_j, \wp_j)$;

  else

  res=res $\cup$ *ZeroDecGTZ(*U_j*);*

- *return res.*

Higher Dimensional Primary Decomposition

The following proposition tells how to adapt the primary decomposition of an arbitrary module to the zero dimensional case.

Proposition 1.2.7. *Let* $U \subset \mathbb{F}[\xi]^s$ *be a module and* $v \subset \xi := \{\xi_1, \dots, \xi_n\}$ *be a maximal independent set modulo* U*. Then:*

1. $\mathbb{F}(v)[\xi \setminus v]U \subset \mathbb{F}(v)[\xi \setminus v]^s$ *is a zero dimensional module.*

2. *Let* $S = \{h_1, \dots, h_s\} \subset U \subset \mathbb{F}[\xi]^s$ *be a Gröbner basis of* $\mathbb{F}(v)[\xi \setminus v]U$*, and let* $g := lcm(lc(h_1), \dots, lc(h_s)) \in \mathbb{F}(v)$*, then* $\mathbb{F}(v)[\xi \setminus v]U \cap \mathbb{F}[\xi] = U : g^\infty$ *and this module is equidimensional to* $\dim U$*.*

3. *Let* $\mathbb{F}(v)[\xi \setminus v]U = \Theta_1 \cap \Theta_2 \dots \cap \Theta_s$ *be an irredundant primary decomposition, then* $\mathbb{F}(v)[\xi \setminus v]U \cap \mathbb{F}[\xi] = (\Theta_1 \cap \mathbb{F}[\xi]) \cap (\Theta_2 \cap \mathbb{F}[\xi]) \dots (\Theta_s \cap \mathbb{F}[\xi])$ *is also an*

irredundant decomposition.

The following algorithm gives a primary decomposition for higher dimensional modules.

Algorithm 1.2.8. ***PrimDecGTZ(*** U ***)***

Input: *a submodule* $U \subseteq V$

Output: *a set of pairs* $(\Theta_i, \wp_i)$ *containing all primary components* Θ_i *of* U *and* $\wp_i = \sqrt{\Theta_i}, i = 1, 2, \ldots, r$ *is prime associated to* Θ_i*;*

- *take a maximal independent set* $v \subset \xi$ *with respect to* U*;*
- *set ring to* $\mathbb{F}(v)[\xi \setminus v]$ *and*

  – *compute a Gröbner basis* $S = \{h_1, h_2, \ldots, h_s\}$ *of* U *with respect to ordering* ℓp *with* $\xi \setminus v >_{\ell p} v$ *in* $\mathbb{F}(v)[\xi \setminus v]$*;*

  –$f := \prod_{i=1}^{s} lc(h_i) \in \mathbb{F}(v)$*, where we take the leading coefficients* $lc(h_i)$ *in field* $\mathbb{F}(v)$*;*

  –*compute* m *such that* $\langle h_1, h_2 \ldots, h_s\rangle : \langle f^m\rangle = \langle h_1, h_2 \ldots, h_s\rangle : \langle f^{m+1}\rangle$*;*

  –*set* $\{(U_i, \wp_i)\}$:=*ZeroDecGTZ*$(\langle S\rangle_{\mathbb{F}(v)[\xi\setminus v]})$*;*

  –$U_i := U_i \cap V$*;*

- *change ring to* $\mathbb{F}[\xi]$ *and compute*

  $prim := \{(U_i, \wp_i)\} \cup PrimDecGTZ(\langle U + f^m.V\rangle)$*;*

- *return prim.*

1.3 The Methods of Eisenbud, Huneke and Vasconcelos

Primary decomposition algorithms of Eisenbud et al. (cf.[EHV92]) for submodules of free modules over polynomial ring $\mathbb{F}[\xi_1, \xi_2, \ldots, \xi_n]$, where $\mathbb{F}$ is a field of rational numbers, are described in detail which are programmed for the computer algebra system SINGULAR(included in appendix), as well as providing proofs of many important theorems of Eisenbud et al's paper. These main ideas depend on the use of homological methods for the equidimensional decomposition of a module and the technique of localization of a module at a prime ideal. Note that all modules are finitely generated.

1.3.1 The Equidimensional Hull of a Submodule

Definition 1.3.1. The *equidimensional hull* of 0 in a module V is defined to be the submodule U such that $U := \{m \in V \mid \dim(0 : m) < \dim V\}$; it can also be defined as a module U which is intersection of all primary components of 0 in V having maximal dimension. If $U \subset V$ is a submodule, The *equidimensional hull* of U is defined to be the preimage in V of the *equidimensional hull* of 0 in V/L. It is denoted by $\mathrm{hull}(U, V)$, or simply by $\mathrm{hull}\, U$ when there is no chance of ambiguity.

Theorem 1.3.1. *Let V be a module over regular domain Ω, and let $l_c = ann\mathrm{Ext}_\Omega{}^c(V, \Omega)$:*

1 . *l_c has codimension $\geq c$ and $V/(0 :_V l_c)$ has no associated primes of codimension c. In particular V has an associated prime ideal $\wp$ of codimension c iff $\wp$ contains the annihilator of $\mathrm{Ext}^c_\Omega(V, \Omega)$.*

2 . *The equidimensional hull of 0 in V is the kernel of the natural map $\pi : V \to$*

$\mathrm{Ext}_\Omega{}^c(\mathrm{Ext}_\Omega{}^c(V,\Omega),\Omega)$, *where* c *is the codimension of* V.

The Theorem 1.3.1 can be used to find the equidimensional hull of a module, or to compute a module U which is intersection of the primary components of V with dimension greater than or equal to any given number.

Algorithm 1.3.2. RemoveComp(V, c)

Input: *a module* V *over ring* $\Omega := \mathbb{F}[\xi_1, \xi_2, ..., \xi_n]$, *and an integer* c *(usually taken* $\geq \dim V$ *)*

Output: *a submodule* U *which is intersection of the primary components of* V *having dimension greater than or equal to* c.

- *set* $h := \dim \Omega$;
- *take* $U := 0 \subset V$;
- *while* $h > c$

  compute $\mathrm{Ext}^h(V,\Omega)$;

  if $(\mathrm{codim}\,\mathrm{Ext}^h(V,\Omega) = h)$

  set $l_h := annihilator(\mathrm{Ext}^h(V,\Omega))$;

  $U := (U :_V l_h)$;

  $h := h - 1$;
- *return the module* U.

Algorithm 1.3.3. EquidimHull*(*V*)*

Input: *a finitely generated module* V *over* $\Omega = \mathbb{F}[\xi_1, \xi_2, \ldots \xi_n]$

Output: The equidimensional hull of 0 *in module* V*.*

- *set* $c := \operatorname{codim} V$*;*
- *compute the module* U*=kernel* $V \to \operatorname{Ext}_\Omega{}^c(\operatorname{Ext}_\Omega{}^c(V, \Omega), \Omega)$*;*
- *return the module* U*.*

1.3.2 Localizations and Primary Decomposition

Let Ω be an affine ring and $l \subset \Omega$ be an ideal, and $U \subset V$ be finitely generated Ω modules. The localization of U at the ideal l, denoted by U_l, is defined as $U_{[l]} = \{m \in V \mid \dim(l + (U : m)) < \dim l\}$. If l is a prime ideal then we can write as $U_{[l]} = \{m \in V \mid (U : b) \subsetneq l\}$.

The following proposition is helpful in actual computation of localization of a module at an ideal.

Proposition 1.3.4. *Let* Ω *be a noetherian ring and* l *be an ideal in* Ω*,and let* $U \subset V$ *be* Ω*-modules, and* l_c *denotes the intersection of all the associated primes of* V/U *which have codimension* c*. If we set*

$$L := \bigcap_c (l_c, (l_c)_l)$$

then

$$U_{[l]} = (U : L^\infty)$$

Theorem 1.3.5. *Let* $U \subseteq \Omega[\xi]^s$ *be a module,* $\wp \in Ass(V)$*. Then* $U + \wp^m \Omega^s$ *is a* $\wp$*–primary component of* U *for some* m*.*

Proof. Let $U = \Theta_1 \cap \Theta_2 \ldots \cap \Theta_s \cap \Theta_{s+1} \ldots \Theta_m$, $\wp = \sqrt{\Theta}$, $\Theta = \Theta_i$. Choose m such that $\wp^m \Omega^s \subseteq \Theta$. Now we can prove that $U + \wp^m \Omega^s \subseteq \cap_{\wp \subseteq \sqrt{\Theta_j}} \Theta_j$, for if $f \in U + \wp^m \Omega^s$, so f is of the form $f = f_1 + f_2$, this implies $f_1 \in \Theta_j$ for any j, and $f_2 \in \Theta_j$, $\wp \subseteq \sqrt{\Theta_j}$, so $f \in \cap_{\wp \subseteq \sqrt{\Theta_j}} \Theta_j$, (as hull$(\cap_{\wp \subseteq \sqrt{\Theta_j}} \Theta_j = \Theta)$) so $hull(U + \wp^m \Omega^s) = \Theta$. So Θ is $\wp$-primary. □

Theorem 1.3.6. *Let $U = \Theta_1 \cap \Theta_2 \cap \ldots \Theta_m$ be an irredundant primary decomposition, $\wp_i = \sqrt{\Theta_i}$. Let $\wp \in \{\wp_1, \wp_2, \ldots, \wp_m\}$ and Θ be a $\wp$–primary module such that $U \subseteq \Theta$. Then Θ is a primary component for U (i.e. there exists i such that $U = \Theta_1 \cap \ldots \Theta_{i-1} \cap \Theta \cap \Theta_{i+1} \ldots \cap \Theta_m$) if and only if $\Theta \cap (U_{[\wp]} : \wp^\infty) = U_{[\wp]}$.*

Proof. Assume $\Theta = \Theta_i$ for some i. Then $\wp = \wp_i$.

Claim. If $\wp$ is not embedded then $U_{[\wp]} = \Theta$ and $U_{[\wp]} : \wp^\infty = \Omega$.

Obviously $U_{[\wp]} \subseteq \Theta$. Let $\xi \in \Theta$ then $U : \xi = (\Theta_1 : \xi) \cap \ldots (\Theta_{i-1} : \xi) \cap (\Theta_{i+1} : \xi) \ldots \cap (\Theta_m : \xi)$. If $(U : \xi) \subseteq \wp = \wp_i$, this implies that $(\Theta_j : \xi) \subseteq \wp_i$ for some $j \neq i$. This implies that $\wp_j \subseteq \wp_i$ which contradicts the assumption that $\wp = \wp_i$ is not embedded. This implies $U : \xi \nsubseteq \wp$ and therefore $\xi \in U_{[\wp]}$. This implies $U_{[\wp]} = \Theta$. Now $\wp^m \subseteq \Theta$ for some m. This implies that $U_{[\wp]} : \wp^\infty = \Omega$ and proves the claim.

Claim.If $\wp_j \subsetneq \wp$ then $U_{[\wp]} : \wp^\infty \subseteq U_{[\wp_j]} \subseteq \Theta_j$.

Let $x \in U_{[\wp]} : \wp^\infty$ i.e. $xq \in U_{[\wp]}$ for all $q \in \wp^m$ for all m. There exists $\lambda \notin \wp, \lambda q x \in U$. Now choose $q \in \wp \setminus \wp_j$ then $\lambda q \notin \wp_j$, this implies $x \in U_{\wp_j}$ and proves the claim. Now let $x \in \Theta \cap (U_{[\wp]} : \wp^\infty)$ then $U : x = (\Theta_1 : x) \cap (\Theta_2 : x) \cap \ldots \cap (\Theta_{i-1} : x) \cap (\Theta_{i+1} : x) \ldots \cap (\Theta_m : x)$. But $x \in U_{[\wp]} : \wp^\infty \subseteq \Theta_j$ for all $\wp_j \subsetneq \wp$. This implies $U : x = \cap_{\wp_j \nsubseteq \Theta_j} \Theta_j : x$. If $U : x \subset \wp$ then $\Theta_j : x \subset \wp$ for some j with $\wp_j \nsubseteq \wp$. But this is not possible. This implies $U : x \nsubseteq \wp$, i.e. $x \in U_{[\wp]}$. Therefore $\Theta \cap (U_{[\wp]} : \wp^\infty) \subseteq U_{[\wp]}$. The other inclusion is obvious. We proved one direction of theorem.

To prove the converse, assume $\wp = \wp_i$ and $\Theta \cap (U_{[\wp]} : \wp^\infty) = U_{[\wp]}$. We proved above that $\Theta_i \cap (U_{[\wp]} : \wp^\infty) = U_{[\wp]}$ Therefore $\Theta \cap (U_{[\wp]} : \wp^\infty) = \Theta_i \cap (U_{[\wp]} : \wp^\infty)$. Let $H = \Theta_1 \cap \ldots \cap \Theta_{i-1} \cap \Theta_{i+1} \ldots \cap \Theta_m$. We have to prove that $V = H \cap \Theta$, i.e. $H \cap \Theta = H \cap \Theta_i$.

Claim $H = V_{[\wp]} : \wp^\infty) \cap (\cap_{\wp_i \not\subseteq \wp} \Theta_i)$.

Let $\xi \in H$, choose m such that $\wp^m \subset \Theta_i$ then $\xi \wp^m \subseteq U \subseteq U_{[\wp]}$. This proves that $H \subseteq U_{[\wp]} : \wp^\infty$. On the other hand we proved already that $U_{[\wp]} : \wp^\infty) \subseteq (\cap_{\wp_i \subseteq \wp} \Theta_i)$. This implies that $U_{[\wp]} : \wp^\infty) \cap (\cap_{\wp_j \not\subseteq \wp} \Theta_j) \subseteq H$. But $H \subseteq U_{[\wp]} : \wp^\infty)$ implies $H = (U_{[\wp]} : \wp^\infty) \cap (\cap_{\wp_j \not\subseteq \wp} \Theta_j)$ and proves the claim. As $\Theta \cap (U_{[\wp]} : \wp^\infty) = \Theta_i \cap (U_{[\wp]} : \wp^\infty)$, so we obtain $H \cap \Theta = H \cap \Theta_i$. □

Example 1.3.7. $l =< x^2, xy >$, $\wp =< x, y >$, $l_{[\wp]} = l$, $l_{[\wp]} : \wp^\infty =< x >$, $\Theta =< x^2, y >$ $\Theta_1 =< x^2, xy, y^2 >$

The above theorem can be restated as:

Theorem 1.3.8. *Let Θ be a $\wp$- primary submodule of $\Omega[\xi]^s$ containing U. Θ is a $\wp$-primary component for U if and only if the natural map*

$$U_{[\wp]} : \wp^\infty / U_{[\wp]} \to \Omega / \Theta$$

is a monomorphism.

Now the algorithm for finding a primary component for a given associated prime is ready.

Algorithm 1.3.9. PrimaryComp$(U, \wp)$

Input: a module $U \subseteq \Omega^s$ and a prime ideal $\wp$.

Output: a primary component Θ of U with associated prime $\wp$.

- *module* $T = \wp\Omega^s$*;*
- *compute* $U_{[\wp]}$*;*
- *compute* $U_{[\wp]} : \wp^\infty$*;*
- *compute* EquidimHull$(U + T)$*;*
- *if* $U_{[\wp]} : \wp^\infty \subset U_{[\wp]}$

  set $\Theta =$ EquidimHull$(U + T)$

  else

  $T = \wp T$
- *return* Θ*.*

Here is the algorithm to find the primary decomposition of a given module.

Algorithm 1.3.10. *(*PrimdecmEHV*(U))*

Input: *a module* $U \subset \Omega[\xi]^s$*, and* $\xi = \{\xi_1, \xi_2, \ldots, \xi_n\}$*.*

Output: *a list* $(\Theta_i, \wp_i)$*, where* Θ_i *is primary component of* U *with associated prime* $\wp_i$*.*

- *compute the module* $V_1 =$ EquidimHull(U)*;*
- *find all minimal associated primes of* $V1$ *i.e* $\min\mathrm{Ass}(\mathrm{Ann}\, U1)$*;*
- *for each* $\wp_i$ *in set* $\min\mathrm{Ass}(U1)$ *compute* $\Theta_i = PrimaryComp(U1, \wp)$*;*
- *set f:=n;*
- *if* U *has embedded primes then*

  while $(f > \mathrm{codim}(U))$

compute $H := \mathrm{Ext}_{\Omega}{}^{f}(U)$

set $l_f := \mathrm{Ann}(H)$

set $c :=$ *codimension*(l_f)

if $(c = f)$

find set $K = \mathrm{minAss}(\textsc{EquidimHull}(l_f))$

compute for each prime ideal $\wp_i$ *in* K, $\Theta_i = \textsc{PrimaryComp}(U, \wp)$

set $f = f - 1$

- *return the set* $(\wp_i, \Theta_i)$.

Chapter 2

On Parallelization of Modular Algorithms

We consider an ideal in a polynomial ring over the rationals. In section 2.1 we describe a parallel modular implementation of the Gröbner basis (resp. standard basis) algorithm. Afterwards we will consider only the case of a zero–dimensional ideal and introduce a parallel modular implementation of the algorithm to compute the associated primes in section 2.2. Finally we give some examples and the corresponding timings in section 2.3. Both algorithms are implemented in SINGULAR. The Gröbner basis resp. standard basis algorithm can be found in the library `modstd.lib` and the algorithm for computing the associated primes in library `assprimeszerodim.lib`.

The task to compute a Gröbner basis (resp. the associated prime ideals of an ideal) consists of two steps. In the first step, we compute the Gröbner basis (resp. the associated prime ideals) modulo p for sufficiently many primes p and use Chinese remainder and Farey fractions to obtain a result over $\mathbb{Q}$. In the second step, we have to verify that the result obtained this way is correct. The second step is usually at least as time consuming as the first step. Omitting the second step would produce a Gröbner basis (resp. the associated prime ideals) only with high probability and the

result could be wrong in extreme situations. It is known that some of the commercial computer algebra systems have problems in this direction.

We use the following notations. Let $X = \{\xi_1, \ldots, \xi_n\}$ be a set of variables. We denote by $\mathbb{Q}[X]$ the polynomial ring over the field of rational numbers in n indeterminates. Given an ideal $l \subseteq \mathbb{Q}[X]$ we can always choose a finite set of polynomials $F_l = \{f_1, \ldots, f_r\}$ such that $l = \langle F_l \rangle$. For a prime number p and $l \subseteq \mathbb{Z}[X]$ we denote $l_p := l \mod p$. If $l = \langle F_l \rangle \subseteq \mathbb{Q}[X]$ and p does not divide the denominators of the coefficients of the f_i we will also write $l_p := \langle f_1 \mod p, \ldots, f_r \mod p \rangle$. Let $S \subseteq \mathbb{F}[X]$ be a set of polynomials, then $\mathrm{LM}(S) := \{\mathrm{LM}(f) \mid f \in S\}$ is the set of leading monomials of S.

2.1 Computing Gröbner bases with modular methods

In the following we consider an ideal $l = \langle F_l \rangle \subseteq \mathbb{Q}[X]$ together with a monomial ordering $>$. Within this section we describe an algorithm for computing a Gröbner basis resp. a standard basis[1] $S \subseteq \mathbb{Q}[X]$ of l by using modular methods. We assume that either l is homogeneous or $>$ is local. We will see that this assumption facilitates the verification step and assures that the result is a Gröbner basis resp. standard basis of l due to Theorem 2.1.3.

The basic idea of the algorithm is as follows. Choose a set P of prime numbers, compute standard bases S_p of $l_p \subseteq \mathbb{F}_p[X]$, for every $p \in P$, and finally lift these modular standard bases to a standard basis $S \subseteq \mathbb{Q}[X]$ of l. The lifting process

[1] For definitions and properties cf. [GP07].

consists of two steps. Firstly, the set $SP := \{S_p \mid p \in P\}$ is lifted to $S_N \subseteq \mathbb{Z}_N[X]$ with $N := \prod_{p \in P} p$ by applying the Chinese remainder algorithm to the coefficients of the polynomials occuring in SP. Since S_N is uniquely determined modulo N we require N to be larger than the moduli of all coefficients occuring in a standard basis of l over $\mathbb{Q}$. Secondly, we obtain $S \subseteq \mathbb{Q}[X]$ by pulling back the modular coefficients occuring in S_N to rational coefficients via the Farey rational map. This map is guaranteed to be bijective provided that $\sqrt{N/2}$ is larger than the moduli of all coefficients in S. This map is defined as :

Definition 2.1.1. The set $F_m := \{a/b \in \mathbb{Q} \mid gcd(a,b) = gcd(b,m) = 1\}$ is called a st of m–th Farey fractions and $f_N := \mathbb{Q}_N \to \mathbb{Z}/\mathbb{N}$ the canonical map defined by $f_N(\frac{a}{b}) = (amodN)(bmodN)^{-1}$ is the Farey Rational map. If $2m^2 < N$ the restriction of f_N to $\mathbb{Q}_N \cap F_m$ is injective.

The latter condition on N concerning the Farey rational map obviously implies the former condition concerning the Chinese remainder algorithm. We consequently define two corresponding notions that are essential regarding the algorithm.

Definition 2.1.2. Let S be a standard basis of l.

1. If S_p is a standard basis of l_p, then the prime number p is called *lucky for* l if and only if $\mathrm{LM}(S) = \mathrm{LM}(S_p)$. Otherwise p is called *unlucky for* l.

2. A set P of lucky primes for l is called *sufficiently large for* l if and only if $\prod_{p \in P} : p \geq \max\{2 \cdot |c|^2 \mid c \text{ coefficient occuring in } S\}$.

Now we can concretize the theoretical idea of the algorithm. Consider a sufficiently large set P of lucky primes for l such that none of these primes divides any coefficient

occuring in F_l, compute the set SP, and lift this result to a rational standard basis S of l as aforementioned. More details can be found in [1].

In practice, we have to handle two difficulties since naturally the standard basis S of l is a priori unknown. In fact, it is necessary to ensure that every prime number used is lucky for l, and to decide whether the chosen set of primes is sufficiently large for l.

Therefore, we fix a natural number s and an arbitrary set of primes P of cardinality s. After having computed the set of standard bases $SP := \{S_p \mid p \in P\}$ we delete the unlucky primes in the following way.

deleteUnluckyPrimes: *We define an equivalence relation on* (P, SP) *by* $(p, S_p) \sim (q, S_q) :\Longleftrightarrow \mathrm{LM}(S_p) = \mathrm{LM}(S_q)$. *Then the equivalence class of largest cardinality is stored in* (P, SP)*, the others are deleted.*

With the aid of this method we are able to choose a set of lucky primes with high probability. A faulty decision will be compensated by subsequent tests. More details and information about the implementation in Singular can be found in [Pf07].

Since we cannot predict if a given set of primes P is sufficiently large for l, we have to proceed by trial and error. Hence, we lift the set SP to $S \subseteq \mathbb{Q}[X]$ as per description at the beginning of this section, and test whether S is already a standard basis of l. Otherwise we enlarge the set P by s new prime numbers and continue analogously until once the test is positive. The test especially implies to verify whether S is a standard basis of $\langle S \rangle$, but this computation in $\mathbb{Q}[X]$ can be very expensive if P is far away from being sufficiently large for l. Hence, we prefix a test in positive characteristic that is a sufficient criterion if P is not sufficiently large for l.

pTestSB: *We randomly choose a prime number* $p \notin P$ *such that* p *does not divide*

the numerator and denominator of any coefficient occuring in F_l. The test is positive if and only if S_p is a standard basis of l_p. We explicitly test whether $F_{l_p} \subseteq \langle S_p \rangle$ and $S_p \subseteq \texttt{std}(l_p)$[2].

This test in positive characteristic accelerates the algorithm enormously. It is much faster than in characteristic zero since the standard basis computation in pTestSB is as expensive as in any other positive characteristic, i.e., as any other standard basis computation within the algorithm.

If the pTestSB is negative, then P is not sufficiently large for l, that is, S cannot be a standard basis of l over $\mathbb{Q}$. Contrariwise, if the pTestSB is positive, then S is most probably a standard basis of l.

Algorithm 2.1.1 shows the modular standard basis algorithm.[3]

Algorithm 2.1.1. modStd(l)

Assume that $l \subseteq \mathbb{Q}[X]$ is homogeneous or $>$ is a local monomial ordering.

Input: $l \subseteq \mathbb{Q}[X]$.

Output: $S \subseteq \mathbb{Q}[X]$ *the standard basis of* l.

- *choose P, a list of primes;*
- $SP = \emptyset$*;*
- *for ($p \in P$) do*

  compute a standard basis S_p of l_p;

  $SP = SP \cup \{S_p\}$*;*

[2]The procedure `std(_)` is implemented in Singular and computes a Gröbner basis resp. standard basis of the input.

[3]The corresponding procedures are implemented in Singular in the library `modstd.lib`.

- $(SP, P) =$ deleteUnluckyPrimes(SP, P)*;*
- *lift* (SP, P) *to* $S \subseteq \mathbb{Q}[X]$ *by applying Chinese remainder and Farey rational map;*
- *if (*pTestSB(l, S, P)*) is positive then*

  if$(l \subseteq \langle S \rangle)$

  if (S *is a standard basis of* $\langle S \rangle$*)*

  return S*;*

  enlarge P*;*
- *return* S*.*

Corollary 2.1.2. *Algorithm* 2.1.1 *can easily be parallelized in the following way:*

(1) Compute the standard bases S_p *in parallel.*

(2) Parallelize the final tests:

- *Check if* $l \subseteq \langle S \rangle$ *by checking if* $f \in \langle S \rangle$ *for all* $f \in F_l$*.*
- *Check if* S *is a standard basis of* $\langle S \rangle$ *by checking if every s–polynomial not excluded by well-known criteria, vanishes by reduction w.r.t.* S*.*

Remark 2.1.1. The presented version of the algorithm is just pseudo-code whereas its implementation in Singular is optimized. E.g., the standard bases S_p of $l_p \subseteq \mathbb{F}_p[X]$ for $p \in P$ are not computed repeatedly, but stored and reused in further iteration steps.

Algorithm 2.1.1 terminates by construction, and its correctness is guaranteed by the following theorem which is proven in [1] resp. [Pf07].

Theorem 2.1.3. *Let $S \subseteq \mathbb{Q}[X]$ be a set of polynomials such that $\mathrm{LM}(S) = \mathrm{LM}(S_p)$ where S_p is a standard basis of l_p for some prime number p, S is a standard basis of $\langle S \rangle$ and $l \subseteq \langle S \rangle$. Then $l = \langle S \rangle$.*

Note that the first condition follows from a positive result of pTestSB whereas the second and third condition are verified explicitly at the end of the algorithm.

Remark 2.1.2. Algorithm 2.1.1 is also applicable for non-homogeneous ideals and arbitrary monomial orderings but then the algorithm is probabilistic, i.e., the output S is a standard basis of the input l only with high probability. More precisely, S is a standard basis of the ideal it generates, $\langle S \rangle$, and includes l, $l \subseteq \langle S \rangle$. To obtain equality one may additionally lift the relations[4] expressing that $l_p = \langle S_p \rangle$. However, experiments indicate that this is much more expensive.

2.2 A modular approach to primary decomposition

Let $\mathbb{F}$ be a perfect infinite field and $l \subseteq \mathbb{F}[X]$ be a zero–dimensional ideal. The following well–known proposition (cf. [GTZ88] or [GP07]) describes how to compute the associated prime ideals of a radical ideal l.

Proposition 2.2.1. *Let $l \subseteq \mathbb{F}[X]$ be a radical ideal.*

1. *Let $l \cap \mathbb{F}[\xi_n] = \langle h \rangle$ and assume $\deg(h) = \dim_{\mathbb{F}} \mathbb{F}[X]/l$. Let $h = h_1 \cdot \ldots \cdot h_s$ be the factorization of h into irreducible factors over $\mathbb{F}$. Then $l = \bigcap_{i=1}^{s} \langle l, h_i \rangle$ and $\langle l, h_i \rangle$ is prime for all i.*

[4] In Singular the command `liftstd`(l, M) computes a standard basis $\{g_1\}\, g_m$ of the ideal $l = \langle f_1, \ldots, f_r \rangle$ together with a matrix M such that $(g_1, \ldots, g_m) = (f_1, \ldots, f_r) \cdot M$.

2. *There exists a non–empty Zariski open subset* $\mathcal{O} \subseteq \mathbb{F}^{n-1}$ *such that for all* $u = (u_1, \ldots, u_{n-1}) \in \mathcal{O}$ *the linear coordinate change* φ_u *defined by* $\varphi_u(\xi_i) = \xi_i$ *for* $i < n$ *and* $\varphi_u(\xi_n) = \xi_n + \sum_{i=1}^{n-1} u_i \xi_i$ *satisfies*

$$\dim_{\mathbb{F}} \mathbb{F}[X]/\varphi_u(l) = \dim_{\mathbb{F}} \mathbb{F}[\xi_n]/(\varphi_u(l) \cap \mathbb{F}[\xi_n]).$$

Corollary 2.2.2. *Let* $F \in \mathbb{F}[T]$, T *a variable, be squarefree and* $r = \xi_n + \sum_{i=1}^{n-1} u_i \xi_i$ *such that* $\deg(F) = \dim_{\mathbb{F}} \mathbb{F}[X]/l$, *and* $F(r) \in l$, *then* l *is a radical ideal. Let* $h = h_1 \cdot \ldots \cdot h_s$ *be the factorization of* h *into irreducible factors over* $\approx$. *Then* $l = \bigcap_{i=1}^{s} \langle l, h_i(r) \rangle$ *and* $\langle l, h_i(r) \rangle$ *are prime for all* i.

Remark 2.2.1. Let $F \in \mathbb{F}[T]$, T a variable, be monic and squarefree, let $r = \xi_n + \sum_{i=1}^{n-1} u_i \xi_i$ such that $\deg(h) = \dim_{\mathbb{F}} \mathbb{F}[X]/l$ and $F(r) \in l$.

1. Let $\varphi : \mathbb{F}[T] \to \mathbb{F}[X]$ be defined by $\varphi(T) = r$. Then $\varphi^{-1}(l) = \langle F \rangle$.

2. Let $\psi : \mathbb{F}[X] \to \mathbb{F}[X]$ be defined by $\psi(\xi_i) = \xi_i, i < n$, and $\psi(\xi_n) = 2\xi_n - r$. Then $\psi(l) \cap \mathbb{F}[\xi_n] = \langle F(\xi_n) \rangle$.

3. Let $\lambda : \mathbb{F}[X]/l \to \mathbb{F}[X]/l$ be the map defined by the multiplication with r, $\lambda(g + l) = r \cdot g + l$. Then F is the characteristic polynomial of λ.

Remark 2.2.1 shows that the approach of Eisenbud, Hunecke, Vasconcelos (cf. [EHV92]) using (1) of the remark, the approach of Gianni, Trager, Zacharias (cf. [GTZ88]) using (2) of the remark and the approach of Monico (cf. [M02]) using (3) of the remark are in principle the same. The computations for (1) resp. (2) require Gröbner bases with respect to suitable block–orderings whereas in (3) we do not need a special ordering for the Gröbner basis but we have to compute a determinant. All three algorithms are implemented in SINGULAR.

Remark 2.2.2. If $\mathbb{F} = \mathbb{C}$ is the field of complex numbers we can use the polynomial F of Corollary 2.2.2 to compute the zeros of the ideal l. The zeros of F are the eigenvalues of the multiplication map λ of remark 2.2.1. Let $\lambda_1, \ldots, \lambda_d$ be the (different) eigenvalues of λ then $l = \bigcap_{i=1}^{d} \langle l, r - \lambda_i \rangle$. $\langle l, r - \lambda_i \rangle$ is a maximal ideal in $\mathbb{C}[X]$ representing a zero of l.

The following proposition (cf. [**?**], [GP07]) is the basis for computing the radical of a zero–dimensional ideal.

Proposition 2.2.3. *Let $l \subseteq \mathbb{F}[X]$ be a zero–dimensional ideal and $l \cap \mathbb{F}[\xi_i] = \langle g_i \rangle$ for $i = 1, \ldots, n$. Let h_i be the squarefree part of g_i. Then $\sqrt{l} = l + \langle h_1, \ldots, h_n \rangle$. If $\deg(f_n) = \dim_{\mathbb{F}} \mathbb{F}[X]/l$ then $\sqrt{l} = \langle l, h_n \rangle$.*

Corollary 2.2.4. *Let $l \subseteq \mathbb{F}[X]$ be a zero–dimensional ideal and $r = \xi_n + \sum_{i=1}^{n-1} u_i \xi_i$. Let $F \in \mathbb{F}[T]$ such that $F(r) \in l$ and $\dim_{\mathbb{F}} \mathbb{F}[X]/l = \deg(F)$. Let h be the squarefree part of F. Then $\sqrt{l} = \langle l, h(r) \rangle$.*

From now on let $\mathbb{F} = \mathbb{Q}$ be the field of rational numbers and $l \subseteq \mathbb{Q}[X]$ be a zero–dimensional ideal. Similarly to section 2.1 we use a test in positive characteristic for the existence of $F \in \mathbb{Q}[T]$ with the properties of Corollary 2.2.4.

pTestRad: *We randomly choose a prime number p such that $d = \dim_{\mathbb{F}_p} \mathbb{F}_p[X]/l_p$ and $u_1, \ldots, u_{n-1} \in \mathbb{F}_p$. Let $r = u_1\xi_1 + \ldots + u_{n-1}\xi_{n-1} + \xi_n$ and φ be defined as in Remark 2.2.1(1). Let $\langle F_p \rangle := \varphi^{-1}(l_p)$. We test if $\deg(F_p) = d$.*

Algorithm 2.2.5 computes the associated primes of l.[5]

Algorithm 2.2.5. assPrimes(l)

[5]The corresponding procedures are implemented in Singular in the library `primdec.lib`.

Input $l \subseteq \mathbb{Q}[X]$ *a zero–dimensional ideal.*

Output $L = \{M_1, \ldots, M_s\}$, M_i *prime and* $\sqrt{l} = \bigcap_{i=1}^{s} M_i$.

- *compute* $S \subseteq \mathbb{Z}[X]$ *a Gröbner basis of* l *with respect to a degree–ordering;*
- *compute* $d = \dim_{\mathbb{Q}} \mathbb{Q}[X]/l$ *using* S*;*
- *if (not* pTestRad(S, d)*)*

  choose P*, a list of primes;*
- *for*$(p \in P)$

  compute monic polynomials $f_i^{(p)}$ *such that* $\langle f_i^{(p)} \rangle = l_p \cap \mathbb{F}_p[\xi_i]$*;*

  lift all $f_i^{(p)}$ *to* $f_i \in \mathbb{Q}[\xi_i]$ *by applying Chinese remainder and Farey rational map;*
- *use* S *to test if* $f_i \in l$*;*
- *if*$(f_i \in l$*for all*$i)$

  then set P *is sufficiently large*

  else

  enlarge P*;*
- *for*$(i = 1, \ldots, n)$

  compute h_i*, the squarefree part of* f_i*;*
- $l = l + \langle h_1, \ldots, h_n \rangle$*;*
- *compute* $S \subseteq \mathbb{Z}[X]$ *a Gröbner basis of* l *with respect to a degree–ordering;*
- *compute* $d = \dim_{\mathbb{Q}} \mathbb{Q}[X]/l$ *using* S*;*

- *choose* $u_i \in \mathbb{Z}$ *randomly,* $r = u_1\xi_1 + \ldots + u_{n-1}\xi_{n-1} + \xi_n$*;*
- *choose* P*, a list of primes;*
- *for* $(p \in P)$

  compute $F^{(p)}$ *monic, squarefree such that* $\deg(F^{(p)}) = d$ *and* $F^{(p)}(r) \in l_p$*;*

  lift all $F^{(p)}$ *to* $F \in \mathbb{Q}[T]$ *by applying Chinese remainder and Farey rational map;*
- *if(*F *is squarefree and* $F(r) \in l$*) then*

  factorize $F = F_1^{\nu_1} \cdots F_s^{\nu_s}$*,* F_i *irreducible;*

  set $L := \{\langle l, F_1(r)\rangle, \ldots, \langle l, F_s(r)\rangle\}$*;*
- *else*

  enlarge P*;*
- *return* L*;*

Corollary 2.2.6. *Algorithm* 2.2.5 *can easily be parallelized by computing the* $f_i^{(p)}$ *resp.* $F^{(p)}$ *parallel. Experiments indicate that the difficult and time consuming part of the algorithm is the test whether* $F(r) \in l$ *and the computation of the* $F_i(r)$*. These can be parallelized, too.*

2.3 Examples and timings

In this section we time the algorithms `modStd` (cf. section 2.1) resp. `assPrimes` (cf. section 2.2) and their parallelizations as opposed to the usual algorithms `std` resp.

for some examples `minAssGTZ`[6] implemented in SINGULAR. Timings are conducted by using the 32-bit version of SINGULAR 3-1-1 on an Intel® Xeon® X5460 with 4 CPUs, 3.16 GHz each, 64 GB RAM under the Gentoo Linux operating system. All examples are chosen from The SymbolicData Project (cf. [G10]).
We choose the following examples to emphasize the superiority of modular standard basis computation and especially its parallelization:

Example 2.3.1. *Characteristic:* 0*, ordering:* `dp`[7]*,* `Cyclic_8.xml` *(cf. [BF91]).*

Example 2.3.2. *Characteristic:* 0*, ordering:* `dp`*,* `Paris.ilias13.xml` *(cf. [KL99]).*

Example 2.3.3. *Characteristic:* 0*, ordering:* `dp`*, homog.* `Cyclic_7.xml` *(cf. [BF91]).*

Example 2.3.4. *Characteristic:* 0*, ordering:* `ds`*,* `Steidel_1.xml` *(cf. [Pf07]).*

Note that in example 2.3.1 resp. 2.3.2 the ideal is neither homogeneous nor is the ordering local. Thus, using `modStd`, we obtain a standard basis only with high probability. Table 2.1 summarizes the results where `modStd`* denotes the parallelized version of the algorithm. In all tables, the symbol "-" indicates out of memory failures. All timings are given in seconds. The basic algorithm `std` runs out of memory for examples 2.3.1 and 2.3.4. As mentioned in section 2.1, it is possible to parallelize the computation in several parts of the algorithm `algmodStd`. In many cases it turns out that the final test - the verification whether the lifted set of polynomials includes the input and is itself a standard basis - is a time consuming part. Therefore we extract the timings for the verification test in Table 2.1, again in seconds. We consider the following examples for the computation of the associated prime ideals of a given zero–dimensional ideal :

[6]The procedure `minAssGTZ(_)` is implemented in SINGULAR in the library `primdec.lib` and computes the minimal associated prime ideals of the input.

[7]*For definitions of the orderings cf. [GP07].*

Example	`std`	`modStd`	`modStd`*
2.3.1	-	4652	2692
2.3.2	35228	861	622
2.3.3	2931	3030	781
2.3.4	-	4	1

Table 2.1: Total running times for computing a standard basis of the considered examples via `std`, `modStd` and its parallelized variant `modStd`*.

Example	verification in `modStd`	verification in `modStd`*
2.3.1	287	73
2.3.2	185	46
2.3.3	2990	746
2.3.4	0	0

Table 2.2: Running times for the verification test in `modStd` and `modStd`*.

Example 2.3.5. *Characteristic:* 0*, ordering:* `dp`*,* `Becker-Niermann.xml` *(cf. [DGP98]).*

Example 2.3.6. *Characteristic:* 0*, ordering:* `dp`*,* `FourBodyProblem.xml` *(cf. [BM10]).*

Example 2.3.7. *Characteristic:* 0*, ordering:* `dp`*,* `Reimer_5.xml` *(cf. [BM10]).*

Example 2.3.8. *Characteristic:* 0*, ordering:* `lp`*,* `ZeroDim.example_12.xml` *(cf. [G10]).*

Example 2.3.9. *Characteristic:* 0*, ordering:* `dp`*,* `Cassou_1.xml` *(cf. [BM10]).*

Using modular methods via the algorithm `assPrimes` we apply all three variants mentioned in section 2.2.

(1) approach of Eisenbud, Hunecke, Vasconcelos (cf. [EHV92]),

(2) approach of Gianni, Trager, Zacharias (cf. [GTZ88]),

(3) approach of Monico (cf. [M02]).

The timings taken by computation are summarized in Table 2.3 and 2.4 where `assPrimes`* denotes the parallelized version of the algorithm. The usual algorithm

Example	`minAssGTZ`	`assPrimes`			`assPrimes`*		
		(1)	(2)	(3)	(1)	(2)	(3)
2.3.5	-	0	0	1	0	0	0
2.3.6	-	139	139	148	96	83	96
2.3.7	-	132	128	175	97	70	103
2.3.8	170	125	125	125	67	68	63
2.3.9	525	112	112	112	56	56	57

Table 2.3: Total running times for computing the associated prime ideals of the considered examples via `minAssGTZ`, `assPrimes` and its parallelized variant `assPrimes`*.

`minAssGTZ` runs out of memory for examples 2.3.5, 2.3.6 and 2.3.7. Analogous to the modular standard basis algorithm, we also list the timings needed for the verification test in `assPrimes` resp. `assPrimes`* in Table 2.4.

Example	verification in `assPrimes`			verification in `assPrimes`*		
	(1)	(2)	(3)	(1)	(2)	(3)
2.3.5	0	0	0	0	0	0
2.3.6	123	123	123	70	70	69
2.3.7	110	109	111	62	61	62
2.3.8	125	124	124	67	67	63
2.3.9	111	111	111	55	56	56

Table 2.4: Running times for the verification test in `assPrimes` and `assPrimes`*.

Chapter 3

Shomoyama and Yokoyama Method for Primary Decomposition

The aim is to generalize the methods of Shimoyama, Yokoyama for primary decomposition of ideals to submodules of modules in Ω^m. The corresponding algorithms are implemented in SINGULAR. The following approach turned proved very efficient. Then minimal associated primes are computed by using [GTZ88] for ideals and use the algorithm of [SY96] to compute the primary modules.

3.1 Localization

Let $\Omega = \mathbb{Q}[\xi]$, $\xi = \{\xi_1, \xi_2, \ldots, \xi_n\}$, be the polynomial ring over the the field of rational numbers $\mathbb{Q}$. Here we will introduce the concept of localization a module at a multiplicatively closed set.

Definition 3.1.1. Let $U \subset V$ be the submodules of a free Ω module and let Γ be a

multiplicatively closed subset of Ω. We define the *localization* of U with respect to Γ as $\{a \in V \mid at \in U \text{ for some } t \in \Gamma \backslash \{0\}\}$ denoted by $\Omega_\Gamma U \cap V$.
For a prime ideal $\wp$, we denote the localization at multiplicatively closed set $\Omega \setminus \wp$ as $\Omega_\wp U \cap V$; and for a multiplicatively closed set $\langle \nu \rangle$, we denote it by $\Omega_\wp \nu \cap V$.

Remark 3.1.1. Let Θ be a $\wp$–primary submodule of a free Ω module and let $\Gamma \neq 0$ be a non–empty multiplicatively closed subset of Ω. If Γ is disjoint to $\wp$ then $\Omega_\Gamma \Theta \cap \Omega^s = \Theta$, otherwise $\Omega_\Gamma \Theta \cap \Omega^s = \Omega^s$.

3.2 Pseudo Primary Decomposition and Extraction

Definition 3.2.1. An ideal l of Ω is said to be a *pseudo primary ideal* if $\sqrt{l}$ is a prime ideal. A submodule $U \subset V \subseteq \Omega^s$ is said to be *pseudo primary submodule* of V if and only if $\mathrm{Ann}(V/U)$ is a pseudo primary ideal of Ω.

Proposition 3.2.1. *Let U be a submodule of $V \subseteq \Omega^s$ which is not a pseudo primary submodule, and let $\aleph$ be a set of primary submodules of V such that $U = \cap_{\Theta \in \aleph} \Theta$, $\wp_1, \wp_2, \ldots, \wp_n$ be all minimal associated prime ideals of* $\mathrm{Ann}(V/U)$. *Suppose there exist finite subsets $\Gamma_1, \Gamma_2, \ldots, \Gamma_r$ which satisfy the conditions*

$$\Gamma_i \cap \wp_i = \emptyset \text{ and } \Gamma_i \cap \wp_j \neq \emptyset \text{ for } i \neq j$$

Then the following holds:

1. *The submodule* $\Omega_{\Gamma_i}U \cap V$ *is a pseudo primary submodule with associated prime* $\wp_i$.

2. *The set* $\aleph_i = \{\Theta \in \aleph \mid \sqrt{\mathrm{Ann}(V/\Theta)} \cap \Gamma_i = \emptyset\}$ *contains all primary components of* $\Omega_{\Gamma_i}U \cap V$.

Proof. To prove (2) note that if $b \in \sqrt{\mathrm{Ann}(V/\Theta)} \cap \Gamma_i \subset \sqrt{\mathrm{Ann}(V/\Theta)} \cap \langle \Gamma_i \rangle \Rightarrow b^n \in \mathrm{Ann}(V/\Theta)$ and $b^n \in \langle \Gamma_i \rangle$, for some n. This implies that $b^n a \in \Theta \ \forall a \in V \Rightarrow a \in \Omega_{\Gamma_i}\Theta \cap V \ \ \forall a \in V \Rightarrow \Omega_{\Gamma_i}\Theta \cap V = V$.
To prove (1) let $\Psi_i = \{\wp \in \mathrm{Ass}(U) \mid \wp \cap \Gamma_i = \emptyset\}$. Each embedded prime of U contains at least one isolated prime of U. Since $\Gamma_i \cap \wp_j \neq \emptyset$, each prime ideal belonging to Ψ_i contains $\wp_i$ since it doesn't contain any of $\wp_j$ *for* $j \neq i$. So $\Omega_{\Gamma_i}U \cap V$ is a pseudo primary submodule. □

Definition 3.2.2. Let U be a submodule of V and let $\mathrm{minAss}(U) = \{\wp_1, \wp_2, \ldots, \wp_r\}$, each finite set Γ_i which satisfies the condition:

$$\Gamma_i \cap \wp_i = \emptyset \text{ and } \Gamma_i \cap \wp_j \neq \emptyset \text{ for } i \neq j.$$

is said to be a *separator* of U with respect to $\wp_i$ and the set $\{\Gamma_1, \Gamma_2, \ldots, \Gamma_r\}$ is said to be a *system of separators for* U.

Corollary 3.2.2. *Using the above notations, we conclude that*

1. $\aleph_1, \aleph_2, \ldots, \aleph_r$ *are disjoint and their associated primes sets* $\Psi_1, \Psi_2, \ldots \Psi_r$ *are also disjoint.*

2. *Each pseudo primary submodule of a module U is determined by module itself and a system of separators.*

Lemma 3.2.3. *Let U be a submodule of $V \subseteq \Omega^s$ over a ring Ω and let Γ be a multiplicatively closed subset of Ω, $s = \prod_{s_i \in \Gamma} s_i$, then there exists an integer k such that $U : s^k = \Omega_s U \cap V = \Omega_\Gamma U \cap V$.*

Proof. Let k be chosen such that $U : s^k = U : s^{k+1}$. We will show that $U : s^k = \Omega_s U \cap V$.

Let $a \in \Omega_\Gamma U \cap V$, it implies $\exists\, b \in \Gamma$ such that $ba \in U \Rightarrow \prod_{t \in \Gamma, t \neq b} ba \in U$. So $a \in (U : s) \subset (U : s^2) \subset \ldots (U : s^k) = (U : s^{k+1})$. For equality we now prove the reverse inclusion, let $f \in (U : s^k) \Rightarrow s^k f \in U \Rightarrow f \in \Omega_s U \cap V = \Omega_\Gamma U \cap V$. □

Lemma 3.2.4. *(cf. [SY96]) Let $U \subseteq V$ be submodules of a free Ω-module and let $f \in \Omega$ such that $U : f^k = U : f^{k+1}$ then U can be splitted as $U = (U : f^k) \cap (U + f^k V)$.*

Theorem 3.2.5. *Let $U \subset V$ be submodules of Ω^s. Let $\mathrm{minAss}(U) = \{\wp_1, \wp_2, \ldots, \wp_r\}$ and $\{\Gamma_1, \Gamma_2, \ldots, \Gamma_r\}$ be a system of separators for U. For each i, let $\overline{\Theta}_i = \Omega_{\Gamma_i} U \cap V$, let $t_i = \prod_{s \in \Gamma_i} s$ and d_i be an integer such that $\Omega_{\Gamma_i} U \cap V = (U : t_i^{d_i})$, then*

$$U = \overline{\Theta}_1 \cap \overline{\Theta}_2 \cap \ldots \cap \overline{\Theta}_r \cap U' \quad (*)$$

where $U' = U + s_1^{d_1} V + \ldots + s_r^{d_r} V$. Moreover, either $U' = V$ or $\dim(\mathrm{Ann}(V/U')) < \dim(\mathrm{Ann}(V/U))$.

Proof. As the ascending chain of submodules, $\{(U : t_i) \subset (U : t_i^2) \subset \ldots\}$ always terminates, so we can always find such an integer d_i. By Lemma 3.2.3, we have $(U : t_i^{d_i}) = \Omega_{t_i} U \cap V = \Omega_{\Gamma_i} U \cap V = \overline{\Theta}_i$. The following claim proves the decomposition

$(*)$.

Claim 1. $t_j^{d_j}V \subseteq (U : t_i^{d_i})\ for\ i \neq j$.

Let $\mathcal{Q}$ be a primary decomposition of U. By Proposition 3.2.1

$\overline{\Theta}_j = \cap_{\Theta\in\mathcal{Q},\mathrm{Ann}(V/\Theta)\cap\Gamma_j=\emptyset}\Theta$. Consider a primary component Θ of $\overline{\Theta_j}$. Then $(\Theta : t_j^{d_j}) \supseteq \overline{\Theta}_j$, for each $j \neq i$, since $\overline{\Theta}_j = (U : t_j^{d_j})$ and Θ contains U. So $\mathrm{Ann}(V/(\Theta : t_j^{d_j})) \subseteq \mathrm{Ann}(V/\overline{\Theta}_j)$. If $(\Theta : t_j^{d_j}) \neq V$, i.e, $t_j \notin \sqrt{\mathrm{Ann}(V/\Theta)}$ then $(\Theta : t_j^{d_j})$ is an $\sqrt{\mathrm{Ann}(V/\Theta)}$ associated primary submodule. Then by considering radicals, $\sqrt{\mathrm{Ann}(V/\Theta)} \supseteq \wp_j = \sqrt{\mathrm{Ann}(V/\overline{\Theta}_j)}$. But $\sqrt{\mathrm{Ann}(V/\Theta)} \cap \Gamma_i \supseteq \wp_j \cap \Gamma_i \neq \emptyset$. This contradicts the fact that Θ belongs to $\aleph_i$. This implies that each primary component Θ in $\overline{\aleph}_i$ contains $t_j^{d_j}V\ for\ j \neq i$. This implies that $\overline{\Theta}_i = (U : t_i^{d_i})$ contains $t_j^{d_j}V$.

Claim 2. $U = (U : t_1^{d_1}) \cap (U : t_2^{d_2}) \cap \ldots \cap (U : t_r^{d_r}) \cap (U + t_1^{d_1}V + \ldots + t_r^{d_r}V)$.

By Lemma we have $U = (U : t_i^{d_i}) \cap (U + t_i^{d_i}V)$, for every i. Substituting U with $(U : t_2^{d_2}) \cap (U + t_2^{d_2}V)$ in the submodule $(U + t_1^{d_1}V)$, we have

$$U = (U : t_1^{d_1}) \cap (((U : t_2^{d_2}) \cap (U + t_2^{d_2}V)) + t_1^{d_1}V)$$

From Claim 1 we know $t_1^{d_1}V \subseteq (U : t_2^{d_2})$. This implies $U = (U : t_1^{d_1}) \cap (U : t_2^{d_2}) \cap (U + t_1^{d_1}V + t_2^{d_2}V)$ since $((U : t_2^{d_2}) \cap (U + t_2^{d_2}V)) + t_1^{d_1}V = (U : t_2^{d_2}) \cap (U + t_1^{d_1}V + t_2^{d_2}V)$.

If we repeat this computation $r - 1$ times, we obtain the required result.

Now we show that $\dim(\mathrm{Ann}(V/U')) < \dim(\mathrm{Ann}(V/U))$ if $U' \neq V$. Now $U \subseteq U'$, so $\mathrm{Ann}(V/U)) \subseteq \mathrm{Ann}(V/U')$. For each minimal prime ideal $\wp'$ of $\mathrm{Ann}(V/U')$, $\wp'$ contains $\sqrt{\mathrm{Ann}(V/U')}$ and so it contains also $\sqrt{\mathrm{Ann}(V/U)} = \wp_1 \cap \wp_2 \ldots \cap \wp_r$, then $\wp'$ contains some $\wp_i$. Moreover, since $s_i \notin \wp_i$, we have $\sqrt{\mathrm{Ann}(V/U')} \subsetneq \wp_i$.

This implies $\wp_i \neq \wp'$ and therefore $\dim(\wp') < \dim(\mathrm{Ann}(V/U)) = max\{\dim(\wp_1),$ $\dim(\wp_2), \ldots, \dim(\wp_r)\}$. Since this relation holds for any minimal prime ideal $\wp'$ of $\mathrm{Ann}(V/U')$, we obtain $\dim(\mathrm{Ann}(V/U')) < \dim(\mathrm{Ann}(V/U))$. □

Definition 3.2.3. Let $U \subseteq V$ be submodules of Ω^s. The decomposition of U, as in Theorem 3.2.5,

$$U = (U : t_1^{d_1}) \cap (U : t_2^{d_2}) \cap \ldots (U : t_r^{d_r}) \cap (U + t_1^{d_1}V + \ldots + t_r^{d_r}V)$$

is said to be *pseudo primary decomposition* of U. Each $\overline{\Theta}_i = (U : t_i^{d_i})$ is said to be a *pseudo primary component* of U and U' is said to be the *remainder* in the pseudo primary decomposition.

Corollary 3.2.6. *When the submodule U has no embedded primary components, the pseudo primary decomposition, except the remainder U', is the primary decomposition of U.*

The following proposition shows that the isolated primary component of a submodule can be extracted from the pseudo primary submodule by the localization technique.

Definition 3.2.4. Let U be a pseudo primary submodule of V with $\sqrt{\text{Ann}(V/U)}=\wp$, then any primary submodule Θ containing U, such that $\sqrt{\text{Ann}(V/\Theta)}=\wp$, is called an *isolated primary component* of U.

Proposition 3.2.7. *Let U be a pseudo primary submodule of V with $\sqrt{\text{Ann}(V/U)}=\wp$ and let Θ be its unique isolated primary component. Let v be a subset of ξ which is maximally independent set with respect to $\wp$. Then $\Theta = \mathbb{Q}(v)[\xi \backslash v]U \cap V$.*

Proof. Here we denote $\mathbb{Q}(v)[\xi \backslash v]$ *by* $\mathbb{Q}_v$. It can be noted that $\mathbb{Q}_v \cap V = \mathbb{Q}[\xi]_{\mathbb{Q}[v]^*}U \cap V$, where $\mathbb{Q}[v]^* = \mathbb{Q}[v] \backslash \{0\}$. Fix a primary decomposition $\Theta, \Theta_1, \Theta_2, \ldots, \Theta_r$ of U. Now $\wp \cap \mathbb{Q}[v]^* = \emptyset$ as v is a maximally independent set with respect to $\wp$, moreover

$| v |= \dim(\wp)$. This implies $\mathbb{Q}[v]\Theta \cap V = \Theta$. It can be easily proved that if Θ is a primary submodule over the ring Ω with associated prime $\wp$ and Γ is a multiplicatively closed subset of Ω such that $\Gamma \cap \wp = \emptyset$ then $\Omega_\Gamma\Theta \cap V = \Theta$, otherwise $\Omega_\Gamma\Theta \cap V = V$. On the other hand for each Θ_i, $\sqrt{\mathrm{Ann}(V/\Theta_i)}$ contains $\wp$ properly, so $| v |= \dim(\wp) > \dim(\sqrt{\mathrm{Ann}(V/\Theta_i)})$. Therefore v is not an independent set with respect to $\sqrt{\mathrm{Ann}(V/\Theta_i)}$ and $\sqrt{\mathrm{Ann}(V/\Theta_i)} \cap \mathbb{Q}_v^* \neq \emptyset$. So we obtain $\mathbb{Q}_v\Theta_i \cap V = V$ and

$$\mathbb{Q}_v U \cap V = (\mathbb{Q}_u\Theta \cap V) \cap (\cap_{i=1}^r(\mathbb{Q}_v\Theta_i \cap V)) = \Theta$$

□

Theorem 3.2.8. *Let $>$ be a module ordering on $\mathbb{Q}[\xi]^s$ induced from a product ordering (cf. [GPS10]) on $\mathbb{Q}[\xi]$ such that $\xi \setminus v >> v$. Let U be a submodule of a free Ω module $V = \Omega^s$ and let $S = \{h_1, h_2, \ldots, h_s\} \subset U$ be a Gröbner basis of $\mathbb{Q}(v)[\xi\backslash v]U$. Let $h := lcm(lc(h_1), lc(h_2), \ldots, lc(h_s)) \in \mathbb{Q}(v)$, then $\mathbb{Q}(v)[\xi\backslash v]U \cap V = (U : h^\infty)$.*

Proof. Obviously $(U : h^\infty) \subset \mathbb{Q}(v)[\xi \setminus v]U$. To prove the inverse inclusion let $f \in \mathbb{Q}(v)[\xi \setminus v]U \cap V \Rightarrow NF(f \mid S) = 0$, where NF denotes the Buchberger normal form in $\mathbb{Q}(v)[\xi\backslash v]$. But according to this algorithm, one has to divide only by the leading coefficients $lc(h_i)\, of\, h_i\, for\, i = 1, 2, \ldots, s$. So we get a standard representation $f = \sum_{i=1}^s c_i h_i\,, with\, c_i \in \mathbb{Q}[\xi]_h$. Therefore $h^m f \in U$ for some m. This proves $\mathbb{Q}(v)[\xi \setminus v]U \cap V \subset (U : h^\infty)$. □

Theorem 3.2.9. *Let $>$ be a module ordering on $\mathbb{Q}[\xi]^s$ induced from a product ordering on $\mathbb{Q}[\xi]$ such that $\xi \setminus u >> u$ and let U be a pseudo primary submodule of $V = \Omega^s$, and let h be an element of $\mathbb{Q}[\xi]$ which is lcm of leading coefficients of Gröbner basis of $\mathbb{Q}(v)[\xi\backslash v]U$, where v is a maximal independent set with respect to $\mathrm{Ann}(V/U)$, and let k be an integer such that $\Omega_h U \cap V = (U : h^k)$ and let $U' = U + h^k V$, then*

$\Theta = \Omega_h U \cap V$, *where* Θ *is the isolated primary component of* U, *and* $U = \Theta \cap U'$. *Moreover, either* $U' = V$ *or* $\dim(\mathrm{Ann}(V/U)) > \dim(\mathrm{Ann}(V/U'))$ *holds.*

Proof. We know $U = (U : h^k) + (U + h^k V)$ and $(U : h^k) = (U : h^{(k+1)})$. Now by the previous theorem, $\Theta = \mathbb{Q}(u)[\xi \setminus u]U \cap V = \Omega_h U \cap V = (U : h^k)$. Thus we have $U = \Theta \cap U'$. If $U' \neq V$ then $U \subset U' \Rightarrow \mathrm{Ann}(V/U) \subset \mathrm{Ann}(V/U')$ and, moreover, $h^k \in \mathrm{Ann}(V/U')$ but $h^k \notin \wp$. We have $\wp = \sqrt{\mathrm{Ann}(V/U)} \subset \sqrt{\mathrm{Ann}(V/U')}$ and from this we have $\dim(\mathrm{Ann}(V/U)) > \dim(\mathrm{Ann}(V/U'))$. □

Definition 3.2.5. Let U be a pseudo primary submodule of V with $\sqrt{\mathrm{Ann}(V/U)}$=$\wp$. The decomposition $U = \Theta \cap U'$ in Theorem 3.2.9 is called *extraction* of Θ from U and U' is called the *remainder in the extraction.* The element h is called *extractor* associated with $\wp$.

3.3 Criteria For Redundant Components

Here we will see that the primary decomposition of a given submodule can be obtained from decomposition of its pseudo primary submodules and its remainders and then we give some useful criterion to eliminate redundant components.

Let $\wp_1, \wp_2, \ldots, \wp_r$ be isolated prime ideals associated to U and let $U = \overline{\Theta}_1 \cap \overline{\Theta}_2 \ldots \cap \overline{\Theta_r} \cap U'$ be a pseudo primary decomposition of U. We choose a reduced primary decomposition $\hat{\aleph}_i$ of $\overline{Q}_i$ and $\hat{\aleph}'$ of U'. Then the union $\hat{\aleph} = \hat{\aleph}_1 \cup \ldots \hat{\aleph}_r \cup \hat{\aleph}'$ is a primary decomposition of U and $\mathrm{Ass}(U)$ is divided into disjoint subsets $\Psi_1, \Psi_2, \ldots, \Psi_r$ and $\mathcal{P}'$.

From $\hat{\aleph}$ we obtain another primary decomposition $\aleph_{red}$ of U by eliminating all redundant components.

Proposition 3.3.1. *Every $\aleph_i$ is a subset of $\aleph_{red}$.*

Proof. Since the set of associated primes of a module is unique, so we have $\mathrm{Ass}(\overline{\Theta}_i) = \Psi_i$. Since $\mathrm{Ann}(V/U')$ contains $s_i^{k_i}$ for $i = 1, 2, \ldots, r$, each isolated prime in $\mathrm{Ass}(U')$ intersects with each Γ_i. This implies that $\mathrm{Ass}(U')$ is disjoint to every Ψ_i. It follows that for each primary component Θ in $\aleph_i$ has a distinct associated prime $\wp$ in Ψ_i. This implies that Θ belongs to $\aleph_{red}$. □

Proposition 3.3.2. *Let $U = \cap_{i=1}^{r} \overline{\Theta_i} \cap U'$ be a pseudo primary decomposition of the submodule U, then the following holds:*

1. *An isolated primary component Θ' of U' belongs to $\aleph_{red}$ if and only if Θ' does not contain $\overline{\Theta}_1 \cap \overline{\Theta}_2 \ldots \cap \overline{\Theta_r}$.*

2. *A primary component of a pseudo primary component $\overline{\Theta'}$ of U' belongs to $\aleph_{red}$ if and only if $\overline{\Theta'}$ does not contain $\overline{\Theta}_1 \cap \overline{\Theta}_2 \ldots \cap \overline{\Theta_r}$.*

Proposition 3.3.3.

1. *An isolated primary component Θ' of U' belongs to $\aleph_{red}$ if and only if $\Theta' \supsetneq \Theta$.*

2. *A primary component of pseudo primary component $\overline{\Theta'}$ of U' belongs to $\aleph_{red}$ if and only if $\overline{\Theta'}$ does not contain Θ.*

Definition 3.3.1. Let U be a submodule of V with a primary decomposition $\hat{\aleph}$. For a prime ideal $\wp$, let $\mathrm{Ass}(U, \wp) = \{\wp' \in \mathrm{Ass}(U) \mid \wp' \subset \wp, \wp' \neq \wp\}$ and for a positive

integer s let $\mathrm{Ass}(U,s) = \{\wp' \in \mathrm{Ass}(U) \mid \dim(\wp') > s\}$. For a subset U of $\mathrm{Ass}(U)$, we denote by U_U the submodule $\cap_{\Theta\in\hat{\aleph},\sqrt{\mathrm{Ann}(V/\Theta)}\subset\wp,\wp\in U}\Theta$. For simplicity, we denote $U_{\mathrm{Ass}(U,\wp)}$ and $U_{\mathrm{Ass}(U,s)}$ by $U_\wp$ and U_s, respectively.

Remark 3.3.1. Let U be a submodule of Ω^s and let U be a subset of $\mathrm{Ass}(U)$. Then U_U does not depend on any particular decomposition of U.

Proposition 3.3.4. *Let L be a submodule of V containing U and* $\mathrm{U} = \{\wp \in \mathrm{Ass}(U) \mid \wp \subset \wp' \, for \, some \, \wp' \in \mathrm{Ass}(L), \wp \notin \mathrm{Ass}(L)\}$. *If $\mathrm{Ass}(U) \cap \mathrm{Ass}(L) = \emptyset$ then L contains U_{U}.*

Proof. Let $\Gamma = \Omega \setminus \cup_{\wp'\in\mathrm{Ass}(L)}\wp'$. As $U \subset L$, so $\Omega_\Gamma U \cap V \subset \Omega_\Gamma L \cap V$, and $\Omega_\Gamma U \cap V = \cap_{\Theta'\in\hat{Q},\sqrt{\mathrm{Ann}(V/\Theta')}\cap\Gamma=\emptyset}\Theta' = \cap_{\Theta'\in\hat{\aleph},\sqrt{\mathrm{Ann}(V/\Theta')}\subset\wp',\wp'\in U}\Theta' = U_U$. As $\mathrm{Ass}(U) \cap \mathrm{Ass}(L) = \emptyset$, so $\Omega_\Gamma L \cap V = L$. So $U_U = \Omega_\Gamma U \cap V \subset L$. □

By the above proposition we get:

Corollary 3.3.5. *Let Θ be a unique primary component of module U which belongs to the primary decomposition $\hat{\aleph}$ of U with associated prime $\wp$ having degree d. Then the following conditions are equivalent:*

1. *Θ belongs to the irredundant primary decomposition $\aleph_{red}$ obtained from $\hat{\aleph}$.*
2. *$\Theta \supsetneq U_\wp$.*
3. *$\Theta \supsetneq U_d$.*

3.4 The Primary Decomposition Procedure

We fix submodules $U \subset V$ of Ω^s. The procedure for the primary decomposition of submodules of free modules consists of the following sub-procedures.

i: Compute a pseudo primary decomposition $\overline{\Theta}_1 \cap \overline{\Theta}_2 \ldots \cap \overline{\Theta}_r \cap U'$ of U.
First we compute the primary decomposition of the radical $\sqrt{\mathrm{Ann}(V/U)} = \wp_1 \cap \wp_2 \cap \ldots \cap \wp_r$. Let $G_1, G_2, \ldots G_r$ be Gröbner bases of $\wp_1, \wp_2, \ldots, \wp_r$ with respect to a fixed ordering $>$ on Ω. We compute a system of separators $\{\Gamma_1, \Gamma_2 \ldots, \Gamma_r\}$. From the system, we compute the pseudo primary components $\{\overline{\Theta}_i = \Omega_{\Gamma_i} U \cap V, i = 1, \ldots, r\}$. If $\sqrt{\mathrm{Ann}(V/U)}$ is a prime ideal, the subprocedure outputs U, which can be considered as the trivial pseudo primary component.

ii: Find the primary components Θ_i of U from pseudo primary components $\overline{\Theta}_i$ by extraction $\overline{\Theta} = \Theta_i \cap U_i'$.

iii: Apply the subprocedures i to iv to each submodule among the submodules U' and U_i' found in subprocedures i and ii, if it is disjoint to V. Then we have a primary decomposition (may not be reduced) $\hat{\aleph}$ of U.

iv: Eliminate all redundant components from $\hat{\aleph}$ using the criteria in the previous section and take the intersection of all the irredundant primary components having same associated prime ideal.

Details of subprocedures i and ii are provided in the subsequent sections.

Procedure 1: Primary Decomposition (U)

Procedure 1.

Input: A set of generators of the modules U and V.

Output: A set $\aleph_{red}$ having pairs $(\Theta, \wp)$ such that $U = \cap_{\Theta \in \aleph_{red}} \Theta$ is an irreducible primary decomposition of U and $\wp = \sqrt{\mathrm{Ann}(V/\Theta)}$ is the associated prime of Θ.

Begin

- $\aleph_{red} := \emptyset$;
- $\Psi = \mathrm{minAss}(U)$[1];
- $\mathcal{PG} :=$ *a set of Gröbner basis of the prime components of* Ψ;
- $(\mathcal{QG}, \mathcal{U}') :=$ Pseudo Primary Decomposition (U, PG);
- *for each* $(\overline{\Theta}, \wp)$ *in* $\mathcal{QG}$ *do*

  $(\Theta, U'') := Extraction\,(\overline{\Theta}, \wp)$;
  $\aleph_{red} := \aleph_{red} \cup \{(\Theta, \wp)\}$;
  If $U' \neq V$ *then*
  $\aleph_{red} := \aleph_{red} \cup$ Primary Decomposition (U');

  If $U'' \neq V$ *then*

  $\aleph_{red} := \aleph_{red} \cup$ Primary Decomposition (U'');

- $\aleph_{red} :=$ *set of irredundant primary components of* U *in* $\aleph_{red}$;

[1] $\mathrm{minAss}(U)$ *is the set of minimal associated primes of the annihilator of* V/U. *This can be computed using primary decomposition for ideals.*

- *Return* $\aleph_{red}$*;*

End

3.5 Pseudo Primary Decomposition

Let U be a submodule of V and let $\text{minAss}(U) = \{\wp_1, \wp_2, \ldots, \wp_r\}$. Let S_i be a Gröbner basis of $\wp_i$ for each i, with respect to a fixed ordering $>$ on Ω. If $r = 1$, then U is a pseudo primary submodule and we are done and for $r > 1$, the procedure below tells how to compute the pseudo primary decomposition of U:

i: Compute a system of separators of U.

Since each $\wp_i$ is a minimal element in $\text{Ass}(U)$, so $S_i \setminus (\wp_j \cap S_i) \neq \emptyset$, so we can construct finite sets Γ_i as follows:

(a) $\Gamma_i = \{s_1, s_2, \ldots, s_{i-1}, s_{i+1}, \ldots, s_r\}$, or

(b) $\Gamma_i = \{\prod_{j\neq i}^{r} s_j\}$,

where s_j is an element chosen from $S_j \setminus (\wp_i \cap S_j)$.

Since S_j is a Gröbner basis of $\wp_j$, to check if an element is in $S_j \setminus \wp_i$ one can compute its normal form with respect to S_i. Γ_i obtained from (a) or (b) turn out to be separator of U with respect to $\wp_i$

ii: Compute the localization $\Omega_{\Gamma_i} U \cap V$, for each i.

We compute $\overline{\Theta}_i := \Omega_{\Gamma_i} U \cap V$ by $(U + (s_{i,1}y_1 - 1)V + \ldots, (s_{i,t}y_t - 1)V) \cap V$, here $\Gamma_i = \{s_{i_1}, s_{i_2} \ldots, s_{i_t}\}$ and $y_1, y_2, \ldots, y_t$ are new indeterminates.

iii: Compute an integer k_i such that $(U : s_i^{k_i}) = \overline{\Theta}_i$; where $s_i = \prod_{t \in \Gamma_i} t$. From Theorem 3.2.5, we have $U = \overline{\Theta}_1 \cap \ldots \overline{\Theta}_r \cap (U + (s_1^{k_1}V + \ldots, (s_r^{k_r}V)$.

Procedure 2: Pseudo Primary Decomposition (U, PG)

Procedure 2.

Input: A set of Gröbner basis for U and V, and the set $\mathcal{PG}$ of Gröbner basis of all the associated primes of the ideal $\sqrt{\mathrm{Ann}(V/U)}$.

Output: A pair $(\mathcal{QG}, U')$ where $\mathcal{QG}$ is a collection of pseudo primary components and U' is the remainder of U.

- *If $\mathcal{PG} = \{\wp\}$ then return $\{U, \wp\}$;*
- $\mathcal{QG} := \emptyset$;
- $U' := U$
- *For each $\wp \in \mathcal{PG}$ do*

  find a separator Γ with respect to $\wp$;

  compute $\overline{\Theta}$:= a generating set of the localization $\Omega_\Gamma U \cap V$;

  $\mathcal{QG} :=$ *$\mathcal{QG} \cup \{(\overline{\Theta}, \wp)\}$;*

$s := \prod_{t\in\Gamma} t$;

find an integer k *such that* $(U : s^k) = \overline{\Theta}$;

compute $U' := U' + s^k V$;

Return $(\mathcal{QG}, U')$;

3.6 Extraction On A Pseudo Primary Submodule

Let U be a pseudo primary submodule of V and $U \neq V$. Suppose that $\sqrt{\mathrm{Ann}(V/U)} = \wp$ is given by a Gröbner basis with respect to an admissible ordering $>$.

i: Find a maximally independent set v of with respect to $\wp$.

We compute a maximally independent set v with respect to the leading ideal of $\wp$ (this is a maximal independent set with respect to $\wp$, cf. [SY96]).

ii: Compute a Gröbner basis G of U' with respect to a block order $>'$, which satisfies $\xi \setminus v >> v$, and compute the extractor h as $lcm\{lc_v(f) \mid f \in G\}$, where

$lc_v(f)$ is the leading coefficient of f taken as an element of $\mathbb{Q}(v)[\xi \backslash v]$ with respect to the restriction of order $>'$ on $\mathbb{Q}[\xi \setminus v]$.

ii: Compute the localization $\Omega_h U \cap V$.

From Theorem 3.2.9, we have $\Theta = \Omega_h U \cap V$, where Θ is an isolated primary component of U.

iv: Compute an integer k such that $\Theta = (U : h^k)$ then $U = \Theta \cap (U + h^k V)$.

Procedure 3: EXTRACTION $(U, \wp)$

Procedure 3.

Input: A pseudo primary submodule U and a Gröbner basis $\wp$ of $\sqrt{\mathrm{Ann}(V/U)}$.

Output: An isolated primary component Θ of the submodule U and the remainder U' of the extraction.

Begin

- *v:= a maximally independent set with respect to $\wp$;*
- *h:= the extractor associated to U and v;*
- *Θ:= a generating set of the localization $\Omega_h U \cap V$;*
- *k:= an integer such that $(U : h^k) = \Theta$;*
- *$U' := \Theta + h^k V$;*

Return (Θ, U');

End

3.7 Termination of the Procedure

Theorem 3.7.1. *Procedure 1 terminates in finitely many steps.*

Proof. To prove it we use induction on the dimension of the ideal $\mathrm{Ann}(V/U)$ whose associated primes correspond to the associated primes of the submodule $U \subset V$. As the ring Ω is noetherian, $\dim(\mathrm{Ann}(V/U))$ is finite.

First we suppose that $\dim(\mathrm{Ann}(V/U)) = 0$. From Theorem 3.2.5 and Theorem 3.2.9, it can be seen that the remainder, say, W in the pseudo primary decomposition and the extraction becomes V. Thus the procedure stops in this case.

Now suppose that $\dim(\mathrm{Ann}(V/U)) > 0$ assuming the procedure (1) terminates for every submodule K with $\dim(\mathrm{Ann}(V/K)) < \dim(\mathrm{Ann}(V/U))$. If a remainder W, i.e either U' or U'', does not intersect with V, we have $\dim(\mathrm{Ann}(V/W)) < \dim(\mathrm{Ann}(V/U))$ from Theorem 3.2.5 and Theorem 3.2.9. By the induction argument, the primary decomposition procedure stops for the remainders. Hence it also stops for U. □

All computations in the following examples are done using the computer algebra system Singular, cf. [GPS10]

Example 3.7.2. *We take the ordering* $>_m = (>, U)$ *on* Ω^3 *(which gives priority to the coefficients)* $X^\alpha e_i >_m X^\beta e_j \Leftrightarrow \xi^\alpha > \xi^\beta$ *or* $e_i > e_j$ *, with* $e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} > e_2 =$

$\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} > e_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$, *with lex in* Ω *with* $x > y$. *Here we find the primary decomposition of the module* $U = \langle \begin{pmatrix} 0 \\ 0 \\ xy^2 - x^2 - xy \end{pmatrix}, \begin{pmatrix} 0 \\ y \\ x \end{pmatrix}, \begin{pmatrix} 0 \\ x \\ xy - x \end{pmatrix}, \begin{pmatrix} x \\ 0 \\ -xy \end{pmatrix} \rangle$ *in the module* $V = \langle \begin{pmatrix} -y \\ y \\ 0 \end{pmatrix}, \begin{pmatrix} 2y^3 - y^2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} x \\ y^2 \\ 0 \end{pmatrix}, \begin{pmatrix} y - y^2 \\ x \\ 0 \end{pmatrix}, \begin{pmatrix} y \\ 0 \\ x \end{pmatrix} \rangle$; *and* $U \subset V$. $\mathrm{Ann}(V/U) = (x^2 - xy^2 + xy)$ *and* $\mathrm{minAss}(\mathrm{Ann}(V/U)) = \{\wp_1, \wp_2\}$, *where* $\wp_1 = (x - y^2 + y)$ *and* $\wp_2 = (x)$; *and* $\Gamma_1 = \{x\}$ *is a separator with respect to* $\wp_1$ *and* $\Gamma_2 = \{x - y^2 + y\}$ *is a separator with respect to* $\wp_2$. *The pseudo primary components are*

$$\overline{\Theta}_1 := \Omega_{\Gamma_1} U \cap V = \langle \begin{pmatrix} y^3 - y^2 \\ y^3 \\ 0 \end{pmatrix}, \begin{pmatrix} x \\ 0 \\ -xy \end{pmatrix}, \begin{pmatrix} x \\ x + y \\ 0 \end{pmatrix}, \begin{pmatrix} -x \\ x \\ x \end{pmatrix} \rangle \text{ and}$$

$$\overline{\Theta}_2 := \Omega_{\Gamma_2} U \cap V = \langle \begin{pmatrix} 0 \\ 2y^3 - y^2 \\ 0 \end{pmatrix}, \begin{pmatrix} x \\ y^2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ x - y^2 + y \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ y \\ x \end{pmatrix} \rangle.$$

As $\overline{\Theta}_1 = (U : x) \cap V$ *and* $\overline{\Theta}_2 = (U : x - y^2 + y) \cap V$, *the remainder is* $U' := U + xU + (x - y^2 + y)U$

$$= \langle \begin{pmatrix} 2y^3 - 2y^2 \\ y^2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 2y^3 - y^2 \\ 0 \end{pmatrix}, \begin{pmatrix} x \\ y^2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ x - y^2 + y \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ y \\ x \end{pmatrix} \rangle.$$

Next we apply the procedure for extraction of the primary components from pseudo primary components. Now $u = \{y\}$ *is the maximal independent set with respect to* $\wp_1$ *and* $\wp_2$*, and* $h_1 = y^3$ *and* $h_2 = 2y^3 - y^2$ *are the corresponding extractors.*

$$\Theta_1 := \Omega_{h_1}\overline{\Theta}_1 \cap V = \langle \begin{pmatrix} y^3 - y^2 \\ y^3 \\ 0 \end{pmatrix}, \begin{pmatrix} x \\ y^2 \\ 0 \end{pmatrix}, \begin{pmatrix} x \\ x + y \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ y \\ x \end{pmatrix} \rangle$$

$$\textit{and } \Theta_2 := \Omega_{h_2}\overline{\Theta}_2 \cap V = \langle \begin{pmatrix} 0 \\ 2y^3 - y^2 \\ 0 \end{pmatrix}, \begin{pmatrix} x \\ y^2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ x - y^2 + y \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ y \\ x \end{pmatrix} \rangle.$$

Moreover$\Theta_1 = (\overline{\Theta}_1 : h_1) \cap V$ *and* $\Theta_2 = (\overline{\Theta}_2 : h_2) \cap V$*, so the remaining components in extraction are*

$$X := \overline{\Theta_1} + h_1 V = \langle \begin{pmatrix} y^3 - y^2 \\ y^3 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 2y^4 - y^3 \\ 0 \end{pmatrix}, \begin{pmatrix} x \\ y^2 \\ 0 \end{pmatrix}, \begin{pmatrix} x \\ x + y \\ 0 \end{pmatrix}, \begin{pmatrix} -x \\ -x \\ x \end{pmatrix} \rangle$$

and

$$Y := \overline{\Theta}_2 + h_2 V$$

$$=\langle \begin{pmatrix} 0 \\ 2y^3-y^2 \\ 0 \end{pmatrix}, \begin{pmatrix} 2y^4-y^3 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} x \\ y^2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ x-y^2+y \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ y \\ x \end{pmatrix} \rangle$$

respectively.

Now $\mathrm{Ann}(V/X) = (y^3, x-y^2+y)$ *which is* $\wp_x = (y,x)$*-primary. So* X *is also* $\wp_x$*-primary by Remark 1.1.2, as* $\wp_x$ *is a maximal ideal.*

Next we compute the primary decomposition of Y*. Now* $\mathrm{Ann}(V/Y) = (2y^3-y^2, x)$ *and* $\mathrm{minAss}(\mathrm{Ann}(V/Y)) = \{\wp_3, \wp_4\}$*, where* $\wp_3 = (x,y)$ *and* $\wp_4 = (x, 2y-1)$ *and the separators are* $\Gamma_3 = \{2y_1\}$ *and* $\Gamma_4 = \{y\}$*, respectively. The pseudo primary components of* Y *are* $\Theta_3 := \Omega_{\Gamma_3}Y \cap V = (Y : 2y-1) \cap V$ *and* $\Theta_4 := \Omega_{\Gamma_4}Y \cap V = (Y : y^2) \cap V$ *such that*

$$\Theta_3 = \langle \begin{pmatrix} 2y^3 \\ -y^2 \\ 0 \end{pmatrix}, \begin{pmatrix} -y^3 \\ y^3 \\ 0 \end{pmatrix}, \begin{pmatrix} x \\ y^2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ x-y^2+y \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ y \\ x \end{pmatrix} \rangle$$

$$\Theta_4 = \langle \begin{pmatrix} y-2y^2 \\ -y+2y^2 \\ 0 \end{pmatrix}, \begin{pmatrix} 2y^3-y^2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} x \\ y^2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ x-y^2+y \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ y \\ x \end{pmatrix} \rangle$$

Since $\wp_3$ *and* $\wp_4$ *are maximal ideals, so* Θ_3 *and* Θ_4 *are primary components of* Y*. The remainder of* Y *becomes*V*.*

Now we proceed towards the primary decomposition of the remainder U' *of* U*.* $\mathrm{Ann}(V/U') =$

(y^2-y, x) *and* $\mathrm{minAss}(\mathrm{Ann}(V/U')) = \{\wp_5 = (x, y), \wp_6 = (x, y-1)\}$ *and the separators are* $\Gamma_5 = \{y-1\}$ *and* $\Gamma_6 = \{y\}$*, respectively. The pseudo primary components are* $\Theta_5 := \Omega_{\Gamma_5} U' \cap V = (U' : y-1) \cap V$

$$= \langle \begin{pmatrix} 0 \\ -y^2+y^2 \\ 0 \end{pmatrix}, \begin{pmatrix} 2y^3-2y^2 \\ y^2 \\ 0 \end{pmatrix}, \begin{pmatrix} x \\ y^2 \\ 0 \end{pmatrix}, \begin{pmatrix} -2y^4+4y^3-2y^2 \\ x+2y^5-y^4-y^3+y \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ y \\ x \end{pmatrix} \rangle$$

and $\Theta_6 := \Omega_{\Gamma_6} U' \cap V = (U' : y) \cap V$

$$= \langle \begin{pmatrix} -y^2+y \\ y+y^2 \\ 0 \end{pmatrix}, \begin{pmatrix} 2y^3-2y^2 \\ y^2 \\ 0 \end{pmatrix}, \begin{pmatrix} x \\ y^2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ x-y^2+y \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ y \\ x \end{pmatrix} \rangle$$

and the remainder $U'' := U' + (y-1)V + yV$ *becomes* V*. As* Θ_5 *and* Θ_6 *both contain* $\overline{\Theta}_1 \cap \overline{\Theta}_2$*, so by Proposition* 3.3.2 Θ_5 *and* Θ_6 *are redundant components. Now* X *is redundant as* $\Theta_1 \cap \Theta_2 \cap \Theta_3 \cap \Theta_4 \subset X$*. Similarly we can see that* Θ_3 *and* Θ_4 *are also redundant modules. So the irredundant primary decomposition is* $U = \Theta_1 \cap \Theta_2$*.*

Using the procedures from the SINGULAR library `mprimdec.lib` we obtain this result as follows (the first entry in the list is the primary module, the second entry is the associated prime):

```
LID"mprimdec.lib";
ring R=0,(x,y),(c,dp);
module U=[0,0,xy2-x2-xy],[0,y,x],[0,x,xy-x],[x,0,-xy];
module V=[-y,y],[2y3-y2],[x,y2],[y-y2,x],[y,0,x];
```

```
primSY(U,V);
[1]:
   [1]:
      _[1]=[x,0,-xy]
      _[2]=[0,x,xy-x]
      _[3]=[y3-y2,y3]
      _[4]=[0,-y,-x]
   [2]:
      _[1]=-y2+x+y
[2]:
   [1]:
      _[1]=[2xy-x]
      _[2]=[x,x+y]
      _[3]=[x,y2]
      _[4]=[-xy,xy]
      _[5]=[0,y,x]
   [2]:
      _[1]=x
```

Example 3.7.3. *We compute the primary decomposition of the module*

$$U = \langle \begin{pmatrix} 0 \\ y \\ x \end{pmatrix}, \begin{pmatrix} 0 \\ x \\ xy - x \end{pmatrix}, \begin{pmatrix} x \\ y^2 \\ 0 \end{pmatrix}, \begin{pmatrix} y \\ 0 \\ x \end{pmatrix} \rangle \text{ in } \Omega^3.$$

We take the ordering $>_m$ *as in the previous example. Now* $\mathrm{Ann}(\Omega^3/U) = (2xy^2 + xy, 2x^2 + xy)$ *and* $\mathrm{minAss}(\mathrm{Ann}(\Omega^3/U)) = \{\wp_1 = (x), \wp_2 = (4x+1, 2y-1)\}$ *and the corresponding separators are* $\Gamma_1 = \{2y-1\}$ *and* $\Gamma_2 = \{x\}$*. Now the pseudo primary submodules are*

$$\overline{\Theta}_1 := \Omega_{\Gamma_1} U = \langle \begin{pmatrix} -y \\ y \\ 0 \end{pmatrix}, \begin{pmatrix} y^2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} x \\ y^2 \\ 0 \end{pmatrix}, \begin{pmatrix} y-x \\ x \\ 0 \end{pmatrix}, \begin{pmatrix} y \\ 0 \\ x \end{pmatrix} \rangle \text{ and}$$

$$\overline{\Theta}_2 := \Omega_{\Gamma_2} U = \langle \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -2 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 4y \\ 0 \\ -1 \end{pmatrix}, \begin{pmatrix} 8x \\ 0 \\ 1 \end{pmatrix} \rangle.$$

The remainder in pseudo primary decomposition is

$$U' := U + x^2\Omega^3 + (2y-1)\Omega^3 = \langle \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 2y-1 \end{pmatrix}, \begin{pmatrix} y \\ 0 \\ x \end{pmatrix} \rangle$$

which is $\wp' = (2y-1, x)$ *primary, as* $\mathrm{Ann}(\Omega^3/U') = \wp'$*. Now we apply the extraction procedure on* $(\overline{\Theta}_1, \wp_1)$*. The maximal independent set with respect to* $\wp$ *is* $u = \{y\}$ *and the extractor is* $h := y^2$*. The extracted primary component is*

$$\Theta_1 := \langle \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ x \end{pmatrix} \rangle$$

and $\Theta_1 = (\overline{\Theta}_1 : y^2)$*, so the remainder in the extraction is*

$$X := \overline{\Theta}_1 + y^2\Omega^3 = \langle \begin{pmatrix} -y \\ y \\ 0 \end{pmatrix}, \begin{pmatrix} y^2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} x \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ y^2 \end{pmatrix}, \begin{pmatrix} -x+y \\ x \\ 0 \end{pmatrix}, \begin{pmatrix} y \\ 0 \\ x \end{pmatrix} \rangle.$$

And $\Theta_2 := \overline{\Theta}_2$ *is a primary submodule of* Ω^3*, as* $\wp_2$ *is a maximal ideal. The module* X *is also a* $\wp$*–primary submodule of* Ω^3*, as* $\wp$ *is a maximal ideal. The primary decomposition is* $U = \Theta_1 \cap \Theta_2 \cap X \cap U'$*. As* $\Theta_1 \cap \Theta_2 \cap X \subset U'$*, so the irredundant primary decomposition is* $U = \Theta_1 \cap \Theta_2 \cap X$*.*

Using SINGULAR we obtain:

```
ring R=0,(x,y),(c,dp);
module U=[0,y,x],[0,x,xy-x],[x,y2],[y,0,x];
list L=primSY(U);
L;
[1]:
   [1]:
      _[1]=[0,0,x]
      _[2]=[0,1]
      _[3]=[1]
   [2]:
      _[1]=x
[2]:
   [1]:
      _[1]=[0,0,y2]
```

```
      _[2]=[0,0,xy]
      _[3]=[0,0,x2]
      _[4]=[0,y,x]
      _[5]=[0,x,-x]
      _[6]=[y,0,x]
      _[7]=[x]
   [2]:
      _[1]=y
      _[2]=x
[3]:
   [1]:
      _[1]=[0,0,2y-1]
      _[2]=[0,0,4x+1]
      _[3]=[0,2,-1]
      _[4]=[2,0,-1]
   [2]:
      _[1]=2y-1
      _[2]=4x+1
```

Appendix

The Procedures for the algorithms of Eisenbud, Huneke and Vasconcelos are included in this Appendix.

```
proc primEHV(module M)
"USAGE: primEHV(id); id= ideal/module,

RETURN: a list K of primary ideals and their associated primes:

@* K[i][1] the i-th primary component of M,

@* K[i][2] the i-th prime component of M.

EXAMPLE: example primEHV; shows an example

"

{

     list Z,L,K,W;

     module H;

     ideal If;

     int i,e,n,c;

     n=nvars(basering);

     e=dim(std(M));

     int f=n;

     module M1=canonMap(M)[1];

     module N1=freemodule(nrows(M));
```

```
module N=N1;
L=minAssGTZ(Ann(M1));
int l = size(L);
for( i=1; i<=l; i++)
{
  K[i] = list();
   K[i][2] =std(L[i]);
   K[i][1] = primaryCom(M1,N1,std(L[i]),L);
}
for(i=1;i<=size(K);i++)
{
   N=intersect(N,K[i][1]);
}
if(reduce(N,std(M))!=0)  //if M has embedded primes then
{
   while(f>n-e)
  {          H=ExtR(f,M);
     If=quotient(H,freemodule(nrows(H)));  //If is ann(H)
     c=n-dim(std(If));
    if(c==f)
    {
       Z=minAssGTZ(equiMaxEHV(If));
       for( i=1; i<=size(Z); i++)
      {
```

```
              W[i] = list();
              W[i][2] =std(Z[i]);
              W[i][1] = primaryCom(M,N1,std(Z[i]),Z);
              N=intersect(N,W[i][1]);
            }
             K=K+W;
          }
          f--;
        }
      }
      return(K);
}
   example
{       "EXAMPLE:"; echo = 2;
       ring s=0,(x,y,z),dp;
       ideal i=x2y,xz2,y2z;
       primEHV(i);
       ring T = 0,(x,y,z),dp;
       module M=[xy,0,yz],[0,xz,z2];
       primEHV(M);
}
    proc canonMap(list l)
"USAGE: canonMap(id); id= ideal/module,
RETURN: a list F, the kernel in two different representations and
```

```
@* the cokernel of the canonical map
      @* C ---> Extĉ_S(Extĉ_S(C,S),S) given by presentations
@* Here C is the S-module (S=basering) given by the
@* presentation defined by id, i.e.  C=R/id resp.  C=Sñ/id
@* c is the codimension of C
@* F[1] is the preimage of the kernel in S resp.  Sñ
@* F[2] is a presentation of the kernel
@* F[3] is a presentation of the cokernel
EXAMPLE: example canonMap; shows an example
"
{
      module M=hash[1];
      int c=nvars(basering)-dim(std(M));
      if(c==0)
     {
        module K=syz(transpose(M));
        module Ke=syz(transpose(K));
        module Co=modulo(syz(transpose(syz(K))),transpose(K));
     }
      else
     {
        int i;
        resolution F=mres(M,c+1);
        module K=syz(transpose(F[c+1]));
```

```
        K=simplify(reduce(K,std(transpose(F[c]))),2);
        module A=modulo(K,transpose(F[c]));
        resolution G=nres(A,c+1);
        for(i=1;i<=c;i++)
       {
          K=lift(transpose(F[c-i+1]),K*G[i]);
       }
        module Ke=modulo(transpose(K),transpose(G[c]));
        module Co=modulo(syz(transpose(G[c+1])),transpose(K)+transpose(G[c]));
     }
      return(list(Ke,Co));
}
    example
{       "EXAMPLE:"; echo = 2;
      ring s=0,(u,v),dp;
      ideal i = u,v;
      canonMap(i);
      ring R = 0,(t,u,v,w),dp;
      ideal J1 = t,u;
      ideal J2 = v,w;
      ideal J = intersect(J1,J2);
      canonMap(J);
      module M = syz(J);
      canonMap(M);
```

```
      ring W = 0,(a,b,c,d),Wp(2,3,5,1);
      ideal J = a-d2,b-d3,c-d5;
      ideal I = eliminate(J,d);
      ring A = 0,(x,y,z),Wp(5,2,3);
     ideal L = imap(W,I);
     ideal L2 = L2̂;
     canonMap(L2);
}
    proc primaryComp(module A, module B, ideal P, list L)
"USAGE:com(id1,id2,P,L);id1=ideal/module,id2=ideal/module ,P prime
@* ideal in the list L of prime ideals
RETURN: returns a primary component of the module A
@* defined by id1 associated
@*to prime ideal P defined by id2
EXAMPLE: example com; shows an example
   {
      module T = P*B;
      module Q;
      module AP = groebner(locm(A,B,P,L));
     {
//...and compute the saturation of the localization w.r.t.  P.
        module AP2 = sat(AP,P)[1];
//As long as we have not found a primary component...
        int isPrimaryComponent = 0;
```

```
        while(isPrimaryComponent!=1)
       {
//...compute the equidimensional part Q of A+Pî...
         Q = canonMap(A+T)[1];
//and check if it is a primary component for P.
         if(isSub(intersect(AP2,Q),AP)==1)
         {
           isPrimaryComponent = 1;
         }
         else
         {
           T = P*T;
         }
       }
      return(Q);
}
example
{       "EXAMPLE:"; echo = 2;
      ring r=0,(u,v),dp;
      module H=u*gen(1)+ v*gen(2),
      u*gen(1)-u2*gen(2);
      list L=minAssGTZ(Ann(H));
      ideal P=u;
      module A=freemodule(nrows(H));
      com(H,A,P,L);
```

```
}

 proc localizem(module A,module B,ideal J,list L)
"USAGE: localizem(id1,id2,id,list); id1= ideal/module,

@* id2=ideal/module,id=prime ideal in a list L.

RETURN: The localization of a module A denoted by id1

@* at the prime ideal J denoted by A_[J] defined as A_[J]=(A:K^(infinity))

@* K is intersection of (I_e:(I_e)_J) over all e, where I_e is

@* intersection of all associated primes of B/A

@* having codimension e, where A is subset of B,are

@* modules over freemodule S.

EXAMPLE: example canonMap; shows an example

"

{

      ideal h=quotient(A,B);

      int n=nvars(basering);

      list LL=L;

      ideal I,G,P,Q;

//assume J is in L

      int i,c;

      list H;

      while(size(L)>0)

     {

        I=L[1];

       L=delete(L,1);

        c=dim(std(I));
```

```
        i=1;
        while i<=size(L))
       {
          if(dim(std(L[i]))==c)
         {
           I=intersect(I,L[i]);
           L=delete(L,i);
            i--;
         }
         i++;
       }
         H[size(H)+1]=I;
     }
      ideal K=ideal(1);
      for(i=1; i<=size(H);i++)
     {
        G=localize(H[i],J,LL);
        P=quotient(H[i],G);
        K=intersect(K,P);
     }
      return(sat(A,K)[1]);
}
example
{      "EXAMPLE:"; echo = 2;
```

```
      ring r=0,(x,y),dp;
      module M=[x2,xy2],[xy,y2];
      module A=freemodule(nrows(M));
      list L=minAssGTZ(Ann(M));
      ideal J=L[2]=y-1;
      localizem(M,A,J,L);
}
proc isSub(module I,module J)
"USAGE: isSub(mod1,mod2); mod1= ideal/module,
@* mod2=ideal/module
RETURN: 1 if I is a submodule of J else 0.
"
{
      int s = size(I);
      for(int i=1; i<=s; i++)
     {
        if(reduce(I[i],std(J))!=0)
       {
          return(0);
       }
     }
      return(1);
}
```

Bibliography

[1] Arnold, E. A.; Modular algorithms for computing Gröbner bases. Journal of Symbolic Computation 35, 403–419 (2003).

[Av77] Avramov,L.:Homology of local flat extensions and complete intersection defects.Math.Ann.228,27–37(1977)

[AM69] M. F. Atiyah, I.G. Macdonald, Introduction to Commutative algebra, Addison-Wesley publishing company, 1969.

[BF91] Björck, G.; Fröberg, G.: A Faster Way to Count the Solution of Inhomogeneous Systems of Algebraic Equations, with Applications to Cyclic n-Roots. Journal of Symbolic Computation 12, 329–336 (1991).

[BM10] Bini, D.; Mourrain, B.: Polynomial test suite. Frisco project (LTR 21.024). http://www-sop.inria.fr/saga/POL/ (2010).

[BW96] Becker, E.; Wörmann, T.: Radical computations of zero-dimensional ideals and real root counting. In: Mathematics and Computers in Simulation 42, 561–569 (1996).

[CLO1] David A.Cox, John Little, Donal O'Shea. (2004). Using Algebraic geometry. Springer, second edition.

[CLO97] D. Cox, J. Little, and D. O'shea. Ideals Varieties and Algorithm. Springer Verlag, second edition, 1997.

[DF99] Dummit David S.and Foote Richard M.,Abstract algebra. 2nd eddition, Wiley 1999.

[DGP98] Decker, W.; Greuel, G.-M.; Pfister, G.: Primary Decomposition: Algorithms and Comparisons. In: Algorithmic Algebra and Number Theory, Springer, 187–220 (1998).

[GPS10] Decker, W.; Greuel, G.-M.; Pfister, G.; Schönemann, H.: SINGULAR 3-1-1 — A computer algebra system for polynomial computations. http://www.singular.uni-kl.de (2010).

[D01] A.Dreyer: Primary decomposition of modules. Diploma Thesis 2001.

[E83] Ebert, G. L.: Some comments on the modular approach to Gröbner bases. ACM SIGSAM Bulletin 17, 28–32 (1983).

[E95] D.Eisenbud. Commutative algebra: with a view toward algebraic geometry. Springer Verlag, New York, 1995.

[EHV92] Eisenbud, D.; Huneke, C.; Vasconcelos, W.: Direct Methods for Primary Decomposition. Inv. Math. 110, 207–235 (1992).

[G94] Gräbe, H.-G.: On lucky primes. Journal of Symbolic Computation 15, 199–209 (1994).

[G10] Gräbe, H.-G.: The SymbolicData Project — Tools and Data for Testing Computer Algebra Software. http://www.symbolicdata.org (2010).

[GP07] Greuel, G.-M.; Pfister, G.: A SINGULAR Introduction to Commutative Algebra. Second edition, Springer (2007).

[GTZ88] Gianni, P.; Trager, B.; Zacharias, G.: Gröbner Bases and Primary Decomposition of Polynomial Ideals. Journal of Symbolic Computation 6, 149–167 (1988).

[HT1] Jurgen Herzog, Takayuki Hibi. Monomials. Preprint, Springer, Dec 2008.

[Id09] Idrees, N.: Algorithms for Primary Decomposition of Modules. Studia. Sci. Math. Hungarica, Dec 2009.

[IPS10] Idrees, N., Pfister, G., Steidel S.: Parallelisation of Modular Algorithms. Journal of Symbolic Computation(submitted), May 2010.

[KG83] Kornerup, P.; Gregory, R. T.: Mapping Integers and Hensel Codes onto Farey Fractions. BIT 23(1), 9–20 (1983).

[KL91] Krick, T.; Logar, A.: An Algorithm for the Computation of the Radical of an Ideal in the Ring of Polynomials. AAECC9, Springer LNCS 539, 195–205 (1991).

[KL99] Kotsireas, I.; Lazard, D.: Central Configurations of the 5-body problem with equal masses in three-dimensional space. Representation theory, dynamical systems, combinatorial and algorithmic methods. Part IV, Zap. Nauchn. Sem. POMI, 258, POMI, St. Petersburg, 292-317 (1999).

[M02] Monico, C.: Computing the Primary Decomposition of zero–dimensional Ideals. Journal of Symbolic Computation 34, 451–459 (2002).

[Pa92] Pauer, F.: On lucky ideals for Gröbner bases computations. Journal of Symbolic Computation 14, 471–482 (1992).

[Pf07] Pfister, G.: On Modular Computation of Standard bases. Analele Stiintifice ale Universitatii Ovidius, Mathematical Series XV (1), 129–137 (2007).

[Ru92] E.W.Rutman: Gröbner bases and primary decomposition of modules. J. Symbolic Computation (1992)14, 483-503.

[ST89] Sasaki, T.; Takeshima, T.: A modular method for Gröbner-basis construction over $\mathbb{Q}$ and solving system of algebraic equations. Journal of Information Processing 12, 371–379 (1989).

[SY96] T.Shimoyama, K.Yokoyama: Localization and primary decomposition of polynomial ideals. J. Symbolic Computation (1996) 22, 247-277.

[W87] Winkler, F.: A p–adic approach to the computation of Gröbner bases. Journal of Symbolic Computation 6, 287–304 (1987).