AN ALGORITHM TO COMPUTE A PRIMARY DECOMPOSITION OF MODULES IN POLYNOMIAL RINGS OVER THE INTEGERS

NAZERAN IDREES, GERHARD PFISTER, AND AFSHAN SADIQ

Abstract. We present an algorithm to compute the primary decomposition of a submodule $\mathcal{N}$ of the free module $\mathbb{Z}[x_1,\dots,x_n]^m$. For this purpose we use algorithms for primary decomposition of ideals in the polynomial ring over the integers. The idea is to compute first the minimal associated primes of $\mathcal{N}$, i.e. the minimal associated primes of the ideal $\mathrm{Ann}(\mathbb{Z}[x_1,\dots,x_n]^m/\mathcal{N})$ in $\mathbb{Z}[x_1,\dots,x_n]$ and then compute the primary components using pseudo-primary decomposition and extraction, following the ideas of Shimoyama-Yokoyama. The algorithms are implemented in Singular.

1. Introduction

Algorithms for primary decomposition in $\mathbb{Z}[x_1,\dots,x_n]^m$ have been developed by Seidenberg (cf. [12]) and Ayoub (cf. [2]) and Gianni, Trager and Zacharias (cf. [7]). The method of Gianni, Trager and Zacharias have been generalized by Rutman ([10]) to a submodules of a free module. In our paper we present a slightly different approach using pseudo–primary decomposition, and the extraction of the primary components. We use the computation of minimal associated primes of ideals in $\mathbb{Z}[x_1,\dots,x_n]$ (cf. [9]).

Let us recall the primary decomposition for ideals in $\mathbb{Z}[x]$, $x=(x_1,\dots,x_n)$, since the ideas for submodules of $\mathbb{Z}[x]^m$ are similar. The idea to compute the minimal associated prime ideals of an ideal $I\subseteq\mathbb{Z}[x]$ is the following. We compute a Gröbner basis G of I (cf. Definition 2.2). $G\cap\mathbb{Z}$ generates $I\cap\mathbb{Z}$. If $I\cap\mathbb{Z}=\langle a\rangle$ and $a=p_1^{v_1}\cdot\ldots\cdot p_s^{v_s}$ the prime decomposition then we compute for all i the minimal associated primes of $I\mathbb{F}_{p_i}[x]$, defined by the canonical map $\pi_i:\mathbb{Z}[x]\longrightarrow\mathbb{F}_{p_i}$. If $\overline{P}$ is a minimal associated prime of $I\mathbb{F}_{p_i}[x]$ then $\pi_i^{-1}(\overline{P})$ is a minimal associated prime of I. We obtain all minimal associated primes of I in this way. If $I\cap\mathbb{Z}=\langle 0\rangle$ then we consider the ideal $I\mathbb{Q}[x]$ and compute its minimal associated primes. If $\overline{P}\supset I\mathbb{Q}[x]$ is a minimal associated prime then $\overline{P}\cap\mathbb{Z}[x]$ is a minimal associated prime of I. Using the leading coefficients of a Gröbner basis of $I\mathbb{Q}[x]$ we find $h\in\mathbb{Z}$ such that $I\mathbb{Q}[x]\cap\mathbb{Z}[x]=I:h$ and $I=(I:h)\cap\langle I,h\rangle$. The minimal associated primes of $\langle I,h\rangle$ can be computed as described above.

If we know the minimal associated primes $B=\{P_1,\dots,P_r\}$ of I we can find knowing Gröbner bases of P_i a set of separators $S=\{s_1,\dots,s_r\}$ wiith the property $s_i\notin P_i$ and $s_i\in P_j$ for all $j\neq i$. Using the separators we find pseudo–primary

Date: August 16, 2014.

2000 *Mathematics Subject Classification.* Primary 13P99, 13E05;

Key words and phrases. Gröbner bases, primary decomposition, Primary modules, Associated primes, Pseudo primary, Localization, Extraction.

ideals $Q_i = I : s_i^\infty = I : s_i^{k_i}$, i.e. the radical of Q_i is prime (cf. Definition 3.1), $\sqrt{Q_i} = P_i$. We have

$$I = Q_1 \cap \ldots \cap Q_r \cap \langle I, s_1^{k_1}, \ldots s_r^{k_r} \rangle.$$

To find a primary decomposition we have to continue inductively with $\langle I, s_1^{k_1}, \ldots s_r^{k_r} \rangle$ and find from Q_i the primary ideal of I with associated prime P_i. This is given by so–called extraction lemma (the version for modules is Lemma 3.5. If $Q_i = \overline{Q}_i \cap J$, $\overline{Q}_i$ primary and $\sqrt{\overline{Q}_i} = P_i$, $\mathrm{ht}(J) > \mathrm{ht}(P_i)$, then we can extract the $\overline{Q}_i$ using Gröbner bases with respect to special orderings.

2. Gröbner basis for Modules

Let A be a principal ideal domain. Let $\mathcal{M} = A[x]^m$, $m > 0$ be the free module over the polynomial ring over A, $x = \{x_1, \ldots, x_n\}$ and $\mathbf{e}_1, \ldots, \mathbf{e}_m$ the canonical basis of $\mathcal{M}$. In this section we give basic results about Gröbner bases for modules in $\mathcal{M}$.

A monomial ordering $>$ is a total ordering on the set of monomials $\mathrm{Mon}_n = \{x^\alpha = x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n} | \alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n\}$ in n variables satisfying

$$x^\alpha > x^\beta \Longrightarrow x^\gamma x^\alpha > x^\gamma x^\beta$$

for all $\alpha, \beta, \gamma \in \mathbb{N}^n$. Further more $>$ must be a well–ordering. We extend the notion of monomial orderings to the free module $\mathcal{M}$. We call $x^\alpha \mathbf{e}_i = (0, \ldots, x^\alpha, \ldots, 0) \in \mathcal{M}$.

Definition 2.1. Let $>$ be a monomial ordering on $A[x]$. A (module) monomial ordering or a module ordering on $\mathcal{M}$ is a total ordering $>_m$ on the set of monomials $\{x^\alpha \mathbf{e}_i | \alpha \in \mathbb{N}^n,\ i = 1 \ldots m\}$, which is compatible with the $A[x]$-module structure including the ordering $>$, that is, satisfying

1. $x^\alpha \mathbf{e}_i >_m x^\beta \mathbf{e}_j \Longrightarrow x^{\alpha+\gamma} \mathbf{e}_i >_m x^{\beta+\gamma} \mathbf{e}_j$,
2. $x^\alpha > x^\beta \Longrightarrow x^\alpha \mathbf{e}_i >_m x^\beta \mathbf{e}_i$,

for all $\alpha, \beta, \gamma \in \mathbb{N}^n, i, j = 1, \ldots, r$.

Two module ordering are of particular interest:

$$x^\alpha \mathbf{e}_i > x^\beta \mathbf{e}_j :\Longleftrightarrow i < j \text{ or } (i = j \text{ and } x^\alpha > x^\beta),$$

giving priority to the component, denoted by $(c, >)$, and

$$x^\alpha \mathbf{e}_i > x^\beta \mathbf{e}_j :\Longleftrightarrow x^\alpha > x^\beta \text{ or } (x^\alpha = x^\beta \text{ and } i < j),$$

giving priority to the monomial in $A[x]$, denoted by $(>, c)$.

Now fix a module ordering $>_m$ and denote it also with $>$. Since any vector $f \in \mathcal{M} \setminus \{0\}$ can be written uniquely as

$$f = c x^\alpha \mathbf{e}_i + f^*$$

with $c \in A \setminus \{0\}$ and $x^\alpha \mathbf{e}_i > x^{\alpha^*} \mathbf{e}_j$ for every non-zero term $c^* x^{\alpha^*} \mathbf{e}_j$ of f we can define as $\mathrm{LM}(f) := x^\alpha \mathbf{e}_i$, $\mathrm{LC}(f) := c$, $\mathrm{LT}(f) := c x^\alpha \mathbf{e}_i$ and call it the leading monomial, leading coefficient and leading term [1], respectively, of f. Moreover, for $G \subset \mathcal{M}$ we call

$$L_>(G) := L(G) := \langle \mathrm{LT}(g) \mid g \in G \setminus \{0\} \rangle_{A[x]} \subset \mathcal{M}$$

[1] If we want to hint that we consider f in the ring $A[x]$ we write for the leading term $\mathrm{LT}_{A[x]}(f)$.

the leading submodule of $\langle G\rangle$. In particular, if $\mathcal{N} \subset \mathcal{M}$ is a submodule, then $L_>(\mathcal{N}) = L(\mathcal{N})$ is called the leading module of $\mathcal{N}$.

Definition 2.2. Let $\mathcal{N} \subset \mathcal{M}$ be a submodule. A finite set $G \subset \mathcal{N}$ is called a Gröbner basis of N if and only if $L(G) = L(\mathcal{N})$. G is called a strong Gröbner bases of $\mathcal{N}$, if for any $f \in \mathcal{N}\backslash\{0\}$ there exists $g \in G$ such that $\mathrm{LT}(g)$ divides $\mathrm{LT}(f)$.

Strong Gröbner bases always exist over $A[x]$ (cf. [1]). If A is not a principal ideal domain then this is not true in general.
The concept of a normal form with respect to a given system of elements in $\mathcal{M}$ is the basis of the theory of Gröbner bases. We explain this by giving an algorithm.
For terms $ax^\alpha\mathbf{e}_i$ and $bx^\beta\mathbf{e}_k$, $a, b \in A$, we say $ax^\alpha\mathbf{e}_i$ divides $bx^\beta\mathbf{e}_k$ and write $ax^\alpha\mathbf{e}_i \mid bx^\beta\mathbf{e}_k$ if and only if $i = k$, $a \mid b$ and $x^\alpha \mid x^\beta$.

Algorithm 2.3. $\mathrm{NF}(f|S)$
Input: $S = \{f_1, \ldots, f_m\} \subseteq \mathcal{M}$, $f \in \mathcal{M}$.
Output: $r \in \mathcal{M}$ the normal form $NF(f|S)$ with the following properties: $r = 0$ or no monomial of r is divisible by a leading monomial of an element of S. There exist a representation (standard representation) $f = \sum_{i=1}^m \xi_i f_i + r$, $\xi_i \in A[x]$ such that $\mathrm{LM}(f) \geq \mathrm{LM}(\xi_i f_i)$.

- **if** $f = 0$ **then**
  - **return** f;
- $T := \{g \in S\ ,\ \mathrm{LT}(g) \mid \mathrm{LT}(f)\}$;
- **while** $(T \neq \emptyset$ and $f \neq 0)$ **do**
  - choose $g \in T,\ \mathrm{LT}(f) = h\,\mathrm{LT}(g)$;
  - $f := f - hg$;
  - $T := \{g \in S\ , \mathrm{LT}(g) \mid \mathrm{LT}(f)\}$;
- **if** $f = 0$ **then**
  - **return** f;
- **return** $(\mathrm{LT}(f) + NF(f - \mathrm{LT}(f)|S))$;

3. Primary Decomposition for Modules

First we introduce the notion of a pseudo–primary submodule and show how to decompose a module as intersection of pseudo–primary modules. Then we show how to extract the primary decomposition from a pseudo–primary module.

Definition 3.1. An ideal I of $\mathbb{Z}[x]$ is called a pseudo primary ideal if $\sqrt{I}$ is a prime ideal. A submodule $\mathcal{N} \subset \mathcal{M}$ is called a pseudo primary resp. primary submodule of $\mathcal{M}$ if $\mathrm{Ann}(\mathcal{M}/\mathcal{N})$ is a pseudo primary resp. primary ideal of $\mathbb{Z}[x]$.

Definition 3.2. Let $\mathcal{N}$ be a submodule of $\mathcal{M}$ and let $B = \{P_1, P_2, \ldots, P_r\}$ be the set of minimal associated primes. A set $S = \{s_1, \ldots, s_r\}$ is called a system of separators for B if $s_i \notin P_i$ and $s_i \in P_j$ for $j \neq i$.

Lemma 3.3 (Pseudo–Primary Decomposition). *Let $\mathcal{N} \subseteq \mathcal{M}$ be submodule, $B = \{P_1, \ldots, P_r\}$ be the set of minimal associated primes and $S = \{s_1, \ldots, s_r\}$ a system of separators for B. Let*

$$Q_i = N : s_i^\infty = N : s_i^{k_i}$$

then Q_i is a pseudo–primary submodule and

$$\mathcal{N} = Q_1 \cap \ldots \cap Q_r \cap \langle \mathcal{N} + \langle s_1^{k_1}, \ldots, s_r^{k_r}\rangle \mathcal{M}\rangle.$$

Proof. $\mathbb{Z}[x]_{s_i}\mathcal{N}\cap\mathcal{M}$ is pseudo–primary submodule with minimal associated prime P_i. We obtain this module as a quotient $\mathcal{N}:s_i^\infty=\mathbb{Z}[x]_{s_i}\mathcal{N}\cap\mathcal{M}$. This proves that Q_i is pseudo–primary

As in the case of ideals we have $\mathcal{N}=Q_1\cap(\mathcal{N}+s_1^{k_1}\mathcal{M})$ (cf. [6]). Assume we have already
$\mathcal{N}=Q_1\cap\ldots\cap Q_{t-1}\cap(\mathcal{N}+\langle s_1^{k_1},\ldots,s_{t-1}^{k_{t-1}}\rangle\mathcal{M})$, $t\le r$ then
$\mathcal{N}=Q_1\cap\ldots\cap Q_t\cap(\mathcal{N}+\langle s_1^{k_1},\ldots,s_t^{k_t}\rangle\mathcal{M})$ since
$(\mathcal{N}+\langle s_1^{k_1},\ldots,s_{t-1}^{k_{t-1}}\rangle\mathcal{M}):s_t^{k_t}=\mathcal{N}:s_k^{k_t}$.
The last equality hold since $(\mathcal{N}:s_i^\infty):s_j^\infty=\mathcal{M}$ if $i\neq j$. $\square$

Definition 3.4. Let $I\subset\mathbb{Z}[x_1,\ldots,x_n]$ be a prime ideal. Let $I\cap\mathbb{Z}=\langle p\rangle$ and $\mathbb{F}_p$ the prime field of characteristic p. A subset

$$u\subset x=\{x_1,\ldots,x_n\}$$

is called an independent set (with respect to I) if $I\mathbb{F}_p[x]\cap\mathbb{F}_p[u]=\langle 0\rangle$. An independent set $u\subset x$ (with respect to I) is called a maximal if the number of elements is maximal[2].

Lemma 3.5 (Extraction Lemma)**.** *Let $\mathcal{N}=Q\cap J$ be a pseudo–primary submodule of $\mathcal{M}$ with $\sqrt{\mathrm{Ann}(\mathcal{M}/Q)}=P$ and Q be P–primary with $\mathrm{ht}(\mathrm{Ann}(\mathcal{M}/Q))$ $<\mathrm{ht}(\mathrm{Ann}(\mathcal{M}/J))$. Let $u\subset x$ be a maximal independent set for P. Let $P\cap\mathbb{Z}=\langle p\rangle$ and define $q:=\begin{cases}1 \text{ if } p=0\\ p \text{ if } p>0\end{cases}$. Let $A:=\mathbb{Z}[x]_{\langle p\rangle}$[3]. Then the following holds:*

1. $\mathcal{N}A[x\smallsetminus u]\cap\mathcal{M}=Q$.
2. *Let G be a strong Gröbner basis of $\mathcal{N}$ w.r.t. a block ordering satisfying $(x\smallsetminus u)\mathbf{e}_i\gg u\mathbf{e}_j$. Then G is a strong Gröbner basis of $\mathcal{N}A[x\smallsetminus u]$ w.r.t. the induced ordering for the variables $x\smallsetminus u$.*
3. *Let G be a strong Gröbner basis of $\mathcal{N}$ w.r.t. a block ordering satisfying $(x\smallsetminus u)\mathbf{e}_i\gg u\mathbf{e}_j$, $\mathrm{LT}_{A[x\smallsetminus u]}(g_i)=q^{\nu_i}a_i(x\smallsetminus u)^{\beta_i}\mathbf{e}_j$ with $a_i\in\mathbb{Z}[u]\smallsetminus\langle p\rangle$ for $i=1,\ldots,k$, and $h=\mathrm{lcm}(a_1,\ldots,a_k)$. Then $\mathcal{N}A[x\smallsetminus u]\cap\mathcal{M}=\mathcal{N}:h^\infty$.*

Before proving the lemma let us illustrate it by an example.
Consider the module

$$\mathcal{N}=\langle\begin{pmatrix}0\\0\\xy^2-x^2-xy\end{pmatrix},\begin{pmatrix}0\\y\\x\end{pmatrix},\begin{pmatrix}0\\x\\2xy-x\end{pmatrix},\begin{pmatrix}x\\0\\-xy\end{pmatrix},\begin{pmatrix}0\\0\\18x\end{pmatrix}\rangle,$$

with $\mathcal{N}\subseteq\mathbb{Z}[x.y]^3=\mathcal{M}$.
Let us compute $\mathrm{Ann}(\mathcal{M}/\mathcal{N})=\mathcal{N}:\mathcal{M}$.

```
ring R=integer,(x,y),lp;
module N=[0,0,xy2-x2-xy],[0,y,x],[0,x,2xy-x],[x,0,-xy],[0,0,18x];
ideal I=quotient(N,freemodule(nrows(N)));
I;
I[1]=18x
I[2]=xy2
I[3]=x2-2xy2+xy
```

[2]The number of elements in a maximal independent set u for I is the dimension of $\mathbb{F}_p[x]/I\mathbb{F}_p[x]$.

[3]We are treating the two cases $p=0$ or $p\neq 0$, together. If $p=0$ then $A=\mathbb{F}_p(u)=\mathbb{Q}(u)$ is a field. If $p\neq 0$ then A is a discrete valuation ring with residue field $\mathbb{F}_p(u)$. Especially we have in both cases the existence of strong Gröbner basis over $A[x\smallsetminus u]$.

We can see that $P = \langle x \rangle$ is the only minimal prime associated to I. In this case obviously $u = \{y\}$ is the maximal independent set. We use the following ordering on $\mathbb{Z}[x,y]^3$:
$x^i y^j \mathbf{e}_k > x^l y^m \mathbf{e}_j$ if and only if $i > l$ or $i = l,\ j > m$ or $i = l,\ j = m$ and $k < j$.
Let us compute Gröbner basis with respect to this ordering.

```
std(N);
_[1]=18y*gen(2)
_[2]=y3*gen(2)
_[3]=x*gen(1)+y2*gen(2)
_[4]=x*gen(2)-2y2*gen(2)+y*gen(2)
_[5]=x*gen(3)+y*gen(2)
```

The Gröbner basis is $G = \{ \begin{pmatrix} 0 \\ 18y \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ y^3 \\ 0 \end{pmatrix}, \begin{pmatrix} x \\ y^2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ x - 2y^2 + y \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ y \\ x \end{pmatrix} \}$

Since $P \cap \mathbb{Z} = 0$ we have $\mathbb{Z}[u]_{\langle p \rangle} = \mathbb{Q}(y)$. $\mathcal{N}\mathbb{Q}(y)[x]$ is generated by G which can be simplified to $\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} x \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ x \end{pmatrix}$ since $18y$ is a unit in $\mathbb{Q}(y)$. This implies that $\mathcal{N}\mathbb{Q}(y)[x] \cap \mathbb{Z}[x,y]^3 = \langle \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} x \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ x \end{pmatrix} \rangle$.

We can see this also directly if we compute the Gröbner basis of $\mathcal{N}\mathbb{Q}(y)[x]$ over $\mathbb{Q}(y)[x]$:

```
ring S=(0,y),x,lp;
module N=[0,0,x*y2-x2-x*y],[0,y,x],[0,x,2x*y-x],[x,0,-x*y],[0,0,18x];
std(N);
_[1]=gen(2)
_[2]=x*gen(1)
_[3]=x*gen(3)
```

If we consider the leading terms $\mathrm{LT}_{\mathbb{Z}[x]_{\langle p \rangle}[x \smallsetminus u]}$ of G we obtain $18y\mathbf{e}_2,\ y^3\mathbf{e}_2,\ x\mathbf{e}_1,\ x\mathbf{e}_2,\ x\mathbf{e}_3$, i.e. $a_1 = 18y,\ a_2 = y^3,\ a_3 = 1,\ a_4 = 1,\ a_5 = 1$ and we obtain $h = \mathrm{lcm}(a_1, a_2, a_3, a_4, a_5) = 18y^3$. Let us compute $\mathcal{N} : 18y^3$:

```
setring R;
quotient(N,18y3);
_[1]=gen(2)
_[2]=x*gen(1)
_[3]=x*gen(3)
```

We obtain again $\mathcal{N}\mathbb{Q}(y)[x] \cap \mathbb{Z}[x,y]^3$.
The computation shows that $\mathcal{N} = Q \cap J$ is pseudo–primary with
$Q = \langle \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} x \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ x \end{pmatrix} \rangle$ and $P = \langle x \rangle = \mathrm{Ann}(\mathcal{M}/Q)$. J is computed in the example at the end of the paper.

Proof. of the lemma 3.5

(1) Let $K = \sqrt{\mathrm{Ann}(\mathcal{M}/J)}$ and $\overline{K} = K\mathbb{F}_p[x]$ then[4] $\overline{K} \supsetneq \overline{P} = P\mathbb{F}_p[x]$ since $\mathrm{ht}(\mathrm{Ann}(\mathcal{M}/Q)) < \mathrm{ht}(\mathrm{Ann}(\mathcal{M}/J))$. This implies that $\overline{K} \cap \mathbb{F}_p[u] \neq \langle 0 \rangle$ since $u \subset x$ is maximally independent for $\overline{P}$. Therefore $K \cap (\mathbb{Z}[u] \setminus \langle p \rangle) \neq \langle 0 \rangle$. Thus it holds $JA[x \setminus u] = A[x \setminus u]$. Finally, because Q is primary, we obtain $\mathcal{N}A[x \setminus u] \cap \mathcal{M} = QA[x \setminus u] \cap \mathcal{M} = Q$.

(2) We have to prove that for every $h \in \mathcal{N}A[x \setminus u]$ there exists $g \in G$ such that $\mathrm{LT}_{A[x \setminus u]}(g) \mid \mathrm{LT}_{A[x \setminus u]}(h)$.
Let $h \in \mathcal{N}A[x \setminus u]$. Choose $\eta \in \mathbb{Z}[u] \setminus \langle p \rangle$ such that $\eta h \in \mathcal{N}$. As h is a polynomial in $x \setminus u$ with coefficients in A, the element ηh can be written as

$$\eta h = q^{\nu} a (x \setminus u)^{\alpha} \mathbf{e}_i + (\text{terms in} (x \setminus u)\mathbf{e}_j \text{ of smaller order})$$

with $a \in \mathbb{Z}[u] \setminus \langle p \rangle$.
Since G is a strong Gröbner basis of $\mathcal{N} \subset \mathcal{M}$ there exists a $g \in G$ such that $\mathrm{LT}_{\mathbb{Z}[x]}(g) \mid \mathrm{LT}_{\mathbb{Z}[x]}(\eta h)$.
If $q \neq 1$ and q^{τ} is the maximal power of q dividing the leading coefficient $\mathrm{LC}_{\mathbb{Z}[x]}(g)$ of g then $\tau \leq \nu$ because $\mathrm{LT}(g)$ divide

$$\mathrm{LT}_{\mathbb{Z}[x]}(\eta h) = q^{\nu} \, \mathrm{LT}_{\mathbb{Z}[x]}(a)(x \setminus u)^{\alpha} \mathbf{e}_i.$$

Now we can write g as an element of $F_u[x \setminus u]$ w.r.t. the corresponding ordering, i.e.

$$g = q^{\mu} b (x \setminus u)^{\beta} \mathbf{e}_i + (\text{terms in} (x \setminus u)\mathbf{e}_j \text{ of smaller order})$$

(by assumption G is a strong Gröbner basis of $\mathcal{N}$ w.r.t. a block ordering satisfying $(x \setminus u)\mathbf{e}_i \gg u\mathbf{e}_j$) $b \in \mathbb{Z}[u] \setminus \langle p \rangle$ and $\mu \leq \tau \leq \nu$.
By definition we have

$$\mathrm{LT}_{A[x \setminus u]}(g) = q^{\mu} b (x \setminus u)^{\beta} \mathbf{e}_i$$

resp.

$$\mathrm{LT}_{A[x \setminus u]}(h) = q^{\nu} \frac{a}{\eta} (x \setminus u)^{\alpha} \mathbf{e}_i$$

and on the other hand it holds

$$\mathrm{LT}_{\mathbb{Z}[x]}(g) = q^{\mu} \, \mathrm{LT}_{\mathbb{Z}[x]}(b)(x \setminus u)^{\beta} \mathbf{e}_i$$

resp.

$$\mathrm{LT}_{\mathbb{Z}[x]}(\eta h) = q^{\nu} \, \mathrm{LT}_{\mathbb{Z}[x]}(a)(x \setminus u)^{\alpha} \mathbf{e}_i.$$

Thus the assumption $\mathrm{LT}_{\mathbb{Z}[x]}(g) \mid \mathrm{LT}_{\mathbb{Z}[x]}(\eta h)$ implies $(x \setminus u)^{\beta} \mid (x \setminus u)^{\alpha}$ and consequently $\mathrm{LT}_{A[x \setminus u]}(g) \mid \mathrm{LT}_{A[x \setminus u]}(h)$.

(3) Obviously $(\mathcal{N} : h^{\infty}) \subset A[x \setminus u]\mathcal{N}$. To prove the inverse inclusion let $f \in A[x \setminus u]\mathcal{N} \cap \mathcal{M}$. This implies that $NF(f \mid G) = 0$. But the normal form algorithm requires only to divide by the leading coefficients $\mathrm{LC}(g_i)$ of g_i for $i = 1, 2, \ldots, k$. Hence we obtain a standard representation $f = \sum_{i=1}^{k} c_i g_i$ with $c_i \in \mathbb{Z}[x]_h$. Therefore $h^m f \in \mathcal{N}$ for some m. This proves $A[x \setminus u]\mathcal{N} \cap \mathcal{M} \subset (\mathcal{N} : h^{\infty})$.

$\square$

[4] In case $p = 0$, $\overline{K}$ is the extended ideal $K\mathbb{Q}[x]$. In case $p \neq 0$, $\overline{K}$ is the ideal induced by the canonical map $\mathbb{Z}[x] \longrightarrow \mathbb{F}_p[x]$.

4. The algorithms

In this section we present the algorithm to compute a primary decomposition of a submodule of a free module in a polynomial ring over the integers by applying the results of section 3.

The algorithm to a pseudo–primary component is based on the Pseudo–Primary Lemma 3.3. The algorithm to extract the primary component from the pseudo–primary component is based on the Extraction Lemma 3.5.

Algorithm 4.1. MODPRIMDECZ
Input: $F_{\mathcal{N}} = \{f_1, \ldots, f_k\}$, $\mathcal{N} = \langle F_{\mathcal{N}} \rangle \subseteq \mathbb{Z}[x]^m$.
Output: $K := \{(Q_1, P_1), \ldots, (Q_s, P_s)\}$, $\mathcal{N} = Q_1 \cap \ldots \cap Q_s$ irredundant primary decomposition with $P_i = \sqrt{Q_i}$.

$P := \emptyset$ a list of primary decomposition
$K := \emptyset$ a list of remaining elements
$L := \{(\overline{Q}_1, P_1), \ldots, (\overline{Q}_r, P_r)\} :=$ MODPSEUDOPRIMDECZ$(\mathcal{N})$;
for $i = 1, \ldots, r$ **do**
  if $P_i \neq 0$ **then**
    compute u_i a maximal independent set for P_i;
    $(Q_i, h) :=$ MODEXTRACTZ$((\overline{Q}_i, P_i), u)$;
    $P := P \cup (Q_i, P_i)$;
    $K := K \cup (\overline{Q}_i + h\mathbb{Z}[x]^m)$;
  else
    $P := P \cup (\overline{Q}_i, P_i)$;
for $j = 1, \ldots,$ size(K) **do**
  $S :=$ MODPRIMDECZ(K_j);
  $P := P \cup S$;
return P;

Algorithm 4.2. MODPSEUDOPRIMDECZ

Input: $\mathcal{N}$ a submodule of the free module $\mathcal{M}$.

Output: a list R of pseudo–primary modules of $\mathcal{N}$ and their associated primes.

if $\mathcal{N} = \mathcal{M}$ **then**
  return $\emptyset$
$I := \mathrm{Ann}(\mathcal{M}/\mathcal{N})$;
if $\mathcal{N} = 0$ **then**
  return $(\mathcal{N}, 0)$;
else
  compute $B := \{P_1, \ldots, P_r\}$, the set of minimal associated primes of I;
  comute $\{s_1, \ldots, s_r\}$ a system of separators for B;
  for $i = 1, \ldots, r$ **do**
    compute the saturation Q_i of N w.r.t s_i and the integer k_i, the index of the saturation.
    $R := \{(Q_1, P_1), \ldots, (Q_r, P_r)\}$;
    $L =$ MODPSEUDOPRIMDECZ$(\mathcal{N} + \langle s_1^{k_1}, \ldots, s_r^{k_r} \rangle \mathbb{Z}[x]^m)$;
return $R \cup L$;

Algorithm 4.3. MODEXTRACTZ

Input: K the list of a pseudo–primary module the corresponding minimal associated prime and L is a list of maximal independent set u for the prime ideal.

Output: The primary component Q of $\mathcal{N}$ associated to P and a polynomial h.

$I := \mathrm{Ann}(\mathcal{M}/Q)$;
compute $G = \{g_1, \ldots, g_k\}$, a strong Gröbner basis of $\mathcal{N}$ w.r.t. a block ordering satisfying $x \smallsetminus u \gg u$;
if $I \cap \mathbb{Z} = 0$ **then**
  compute $\{a_1, \ldots, a_k\}$ such that $LC_{\mathbb{Z}(u)[x \smallsetminus u]}(g_i) = a_i$ with $a_i \in \mathbb{Z}[u]$;
  compute $h = lcm(a_1, \ldots, a_k)$, the least common multiple of $a_1, \ldots, a_k$;
if $I \cap \mathbb{Z} = \langle p \rangle$, $p \neq 0$ **then**
  compute $\{a_1, \ldots, a_k\}$ such that $LC_{\mathbb{Z}[u]_{\langle p \rangle}[x \smallsetminus u]}(g_i) = p^{\nu_i} \cdot a_i$ with $a_i \in \mathbb{Z}[u] \smallsetminus \langle p \rangle$;
  compute $h = lcm(a_1, \ldots, a_k)$, the least common multiple of $a_1, \ldots, a_k$;
compute the saturation Q of $\mathcal{N}$ w.r.t h and k, the index of saturation.
return (Q, h^k);

5. Example

We have implemented the algorithms (cf. section 4) in Singular in the library `primdecint.lib` (cf. [4])

Example 5.1.

```
LIB"primdecint.lib";
ring R=integer,(x,y),(c,lp);
module N=[0,0,xy2-x2-xy],[0,y,x],[0,x,2xy-x],[x,0,-xy],[0,0,18x];
> pseudo_primdecZM(N);
[1]:
   [1]:
      _[1]=[0,0,18x]
      _[2]=[0,0,xy2]
      _[3]=[0,0,x2-2xy2+xy]
      _[4]=[0,y,x]
      _[5]=[0,x,2xy-x]
      _[6]=[x,0,-xy]
   [2]:
      _[1]=x

> primdecZM(N);
[1]:
   [1]:
      _[1]=[0,0,x]
      _[2]=[0,1]
      _[3]=[x,0,-xy]
   [2]:
      _[1]=x
[2]:
   [1]:
      _[1]=[0,0,y3]
      _[2]=[0,0,18x]
      _[3]=[0,0,xy2]
      _[4]=[0,0,x2-2xy2+xy]
      _[5]=[0,y,x]
      _[6]=[0,x,2xy-x]
      _[7]=[y3]
      _[8]=[x,0,-xy]
   [2]:
      _[1]=y
      _[2]=x
```

The computation shows that the module $\mathcal{N}$ is pseudo–primary with minimal associated prime $\langle x\rangle$ it has an embedded component with associated prime $\langle x, y\rangle$.

6. Acknowledgement

The authors would like to thank the reviewer for all the useful hints.

References

[1] Adams, W.W.; Loustaunau, P.: An Introduction to Gröbner bases. Graduate studies in mathematics, vol. 3, American Mathematical Scociety, 2003.

[2] Ayoub, C.W.: The Decomposition Theorem for Ideals in Polynomial Rings over a Domain. Journal of Algebra 76, 99–110 (1982).

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

[4] Decker, W.; Greuel, G.-M.; Pfister, G.; Schönemann, H.: Singular 3-1-6 — A computer algebra system for polynomial computations. http://www.singular.uni-kl.de (2013).

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

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

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

[8] Idrees, N.: Algorithms for primary decoposition of modules. Studia Scientiarum Mathematicarum Hungarica 48 (2), 227-246 (2011).

[9] Pfister, G.; Sadiq, A.; Steidel, S.: An Algorithm for Primary Decomposition in Polynomial Rings over the Integers. Central European Journal of Mathematics Vol. 9, No. 4, (2010) 897-904

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

[11] Sadiq, A.: Standard bases over Rings. International Journal of Algebra and Computation, Vol. 20, No. 7 (2010) 953-968.

[12] Seidenberg, A.: Constructions in a Polynomial Ring over the Ring of Integers. American Journal of Mathematics 100 (No. 4), 685–703 (1978).

[13] Shimoyama, T.; Yokoyama, K.: Localization and Primary Decomposition of Polynomial Ideals. Journal of Symbolic Computation 22, 247–277 (1996).

Nazeran Idrees, Department of Mathematics, GC University, Kotwali Road,Jinnah Town, Faisalabad 38000,Punjab, Faisalabad Pakistan,

E-mail address: nazeranjawwad@gmail.com

Gerhard Pfister, Department of Mathematics, University of Kaiserslautern, Erwin-Schrödinger-Str., 67663 Kaiserslautern, Germany

E-mail address: pfister@mathematik.uni-kl.de

URL: http://www.mathematik.uni-kl.de/∼pfister

Afshan Sadiq,, Department of Mathematics,, Jazan University,, P.O. Box 114, Jazan, Saudia Arabia.

E-mail address: afshansadiq6@gmail.com