Algorithm for primary submodule decomposition without producing intermediate redundant components

talk at the

Algebraic Geometry and its applications

Afshan Sadiq

afshanadil@sms.edu.pk

AS-SMS,GC University, Lahore, Pakistan

Outline

- History

Outline

- History
- Task

Outline

- History
- Task
- Basic Definitions and Results

Outline

- History
- Task
- Basic Definitions and Results
- Outline of Algorithm to Compute Primary Decomposition

Outline

- History
- Task
- Basic Definitions and Results
- Outline of Algorithm to Compute Primary Decomposition

History

There are three main algorithms to compute primary decomposition of ideals in polynomial rings over the rational numbers.

- The first algorithm was given by Gianni, Trager, Zacharias. In this algorithm the primary decomposition is done by reducing the problem to the zero-dimensional case.

History

There are three main algorithms to compute primary decomposition of ideals in polynomial rings over the rational numbers.

- The first algorithm was given by Gianni, Trager, Zacharias. In this algorithm the primary decomposition is done by reducing the problem to the zero-dimensional case.

- The method of primary decomposition knowing the isolated prime ideals was given by Shimoyama, Yokoyama. In this method they introduced pseudo–primary ideals and extract the primary components from these ideals. An ideal is pseudo–primary if its radical is a prime ideal.

History

There are three main algorithms to compute primary decomposition of ideals in polynomial rings over the rational numbers.

- The first algorithm was given by Gianni, Trager, Zacharias. In this algorithm the primary decomposition is done by reducing the problem to the zero-dimensional case.

- The method of primary decomposition knowing the isolated prime ideals was given by Shimoyama, Yokoyama. In this method they introduced pseudo–primary ideals and extract the primary components from these ideals. An ideal is pseudo–primary if its radical is a prime ideal.

- The method to compute the primary decomposition without having redundant primary ideals was given by Noro and Kawazoe. They introduced saturated separating ideals, ideals obtained as the quotient of an ideal with its isolated primary component.

History

There are three main algorithms to compute primary decomposition of ideals in polynomial rings over the rational numbers.

- The first algorithm was given by Gianni, Trager, Zacharias. In this algorithm the primary decomposition is done by reducing the problem to the zero-dimensional case.

- The method of primary decomposition knowing the isolated prime ideals was given by Shimoyama, Yokoyama. In this method they introduced pseudo–primary ideals and extract the primary components from these ideals. An ideal is pseudo–primary if its radical is a prime ideal.

- The method to compute the primary decomposition without having redundant primary ideals was given by Noro and Kawazoe. They introduced saturated separating ideals, ideals obtained as the quotient of an ideal with its isolated primary component.

Generalization to modules

- The idea of Gianni, Trager and Zacharias have been generalized by Ruthman to submodules of a free modules of polynomial rings over fields.

Generalization to modules

- The idea of Gianni, Trager and Zacharias have been generalized by Ruthman to submodules of a free modules of polynomial rings over fields.
- The idea of Shimoyama, Yokoyama have been generalized by Idrees to submodules of a free modules of polynomial rings over fields.

Abstract

- we present an algorithm for the primary decomposition of a submodule $\mathbf{N}$ of $\mathbf{M} \subseteq \mathbb{Q}[x_1, \ldots, x_n]^s$. We will use for this purpose the algorithms for primary decomposition for ideals in polynomial rings. We will generalize the method of Kawazoe and Noro to primary decomposition for submodules of free modules.

Basic Definition

- Let I be an ideal of R. A set $\mathcal{Q}$ of primary ideals is called a general primary decomposition of I if $I = \cap_{Q \in \mathcal{Q}} Q$. A general primary decomposition $\mathcal{Q}$ is called a primary decomposition of I if the decomposition $I = \cap_{Q \in \mathcal{Q}} Q$ is a shortest irredundant decomposition.
- Let I be an ideal of R and T a multiplicative closed set in R. We denote the set $\{a \in R \mid ab \in I \text{for some } b \in T\{0\}\}$ by $IR_T \cap R$, and call it the localization of I w.r.t T.

Basic Definition

- An ideal I of R is called a pseudo–primary ideal if $\sqrt{I}$ has a unique prime component, that is, $\sqrt{I}$ is a prime ideal.
- Let I be an ideal of R which is not a pseudo–primary ideal, $P_1, \ldots, P_r$ all isolated prime divisors of I, and $\mathcal{Q}$ a primary decomposition of I. Suppose that there finite subsets $S_1, \ldots, S_r$ in R which satisfy the following conditions:

$$S_i \cap P_i = \emptyset \text{ and } S_i \cap P_j \neq \emptyset \text{ for } i \neq j$$

each S_i is called a separator of I w.r.t P_i.

Pseudo-Primary Decomposition

- Theorem(SY) For each i, let $\overline{Q}_i = IR_{S_i} \cap R$, $s_i = \prod_{s \in S_i} s_i$ and k_i an integer such that $I : s_i^{k_i} = IR_{s_i} \cap R$. Then

$$I = \overline{Q}_1 \cap \ldots \cap \overline{Q}_r \cap I',$$

where $I' = \langle I, s_1^{k_1} \ldots, s_r^{k_r} \rangle$. Moreover, either $I' = R$ or $dim(I') < dim(I)$ holds.

Extraction

- Let I be an ideal in R, Then a subset $u \subset x\{x_1, \ldots, x_n\}$ is called an independent set (w.r.t I) if $I \cap K[u] = 0$. An independent set $u \subset x$ (w.r.t I) is called maximal if $dim(k[x]/I) = \sharp u$.
- Let I be a pseudo-primary ideal with radical P and let Q be its unique isolated primary component. Suppose that a subset u of $x = \{x_1, \ldots, x_n\}$ is maximally independent set module P. Then $Q = I\mathbb{Q}(u)[x \setminus u] \cap R$.

Basic Definition

- Let I, Q be ideals in R satisfying $I \subset Q$. An ideal J is called a separating ideal for (I, Q) if $I = Q \cap (I + J)$ holds. If a separating ideal for (I, Q) satisfies $\sqrt{I : Q} = \sqrt{I + J}$ then J is called a saturated separating ideal for I, Q.
- There exist an integer m satisfying $I = Q \cap (I + (I : Q)^m)$. For such m, $(I : Q)^m$ is a saturated separating ideal. For the same m, $J = \langle f_1^m, \ldots, f_l^m \rangle \subset (I : Q)^m$ is also a saturated separating ideal, where $S = \{f_1, \ldots, f_l\}$ is any generating set of $I : Q$. However from the viewpoint of efficiency it is desirable to find a saturated separating ideal $\langle f_1^{m_1}, \ldots, f_l^{m_l} \rangle$ with each m_i as small as possible.

Proposition

Suppose that $\sqrt{I:Q} = \sqrt{\langle S \rangle}$. If a separating ideal J for $(I:Q)$ satisfies $S \setminus \sqrt{I} \subset \sqrt{I}$, then J is a saturated separating ideal for (I, Q).

Theorem

Let J be a separating ideal for (I, Q). If $f \in \sqrt{I:Q}$ then there exists a positive integer m satisfying $I = Q \cap (I + J + \langle f^m \rangle)$.

Corollary

If $I = Q \cap (I + J)$ and $\sqrt{I+J} \neq \sqrt{I:Q}$ then $(I:Q) \setminus \sqrt{I+J}$, there exists a positive integer m satisfying $I = Q \cap (I + J + \langle f^m \rangle) \neq I + J$.

Basic Definition

- Let $\mathbf{N} \subset \mathbf{Q} \subset \mathbf{M}$ submodules of $\mathbb{Q}[x]^s$. A submodule $\mathcal{K}$ is called a separating submodule for $(\mathbf{N}, \mathbf{Q})$ if

$$\mathbf{N} = \mathbf{Q} \cap (\mathbf{N} + \mathcal{K})$$

holds. If a separating submodule for $(\mathbf{N}, \mathbf{Q})$ satisfies

$$\sqrt{\mathbf{N} : \mathbf{Q}} = \sqrt{\mathrm{Ann}(\mathbf{M}/\mathbf{N} + \mathcal{K})}$$

it is called a saturated separating submodule for $(\mathbf{N}, \mathbf{Q})$.

Proposition

Let $S = \{\xi_1, \ldots, \xi_l\}$ be a generating set for $\mathrm{Ann}(\mathbf{N}/\mathbf{Q})$. If a separating submodule $\mathcal{K}$ satisfies $S \setminus \sqrt{\mathrm{Ann}(\mathbf{M}/\mathbf{N})} \subset \sqrt{\mathrm{Ann}(\mathbf{M}/\mathcal{K})}$, then $\mathcal{K}$ is a saturated separating submodule for $(\mathbf{N}, \mathbf{Q})$

Theorem

Let K be a separating submodule for $(\mathbf{N}, \mathbf{Q})$. If $\xi \in \sqrt{\mathbf{N} : \mathbf{Q}}$, then there exists a positive integer r satisfying $\mathbf{N} = \mathbf{Q} \cap (\mathbf{N} + \mathcal{K} + \xi^r \mathbf{M})$.

Theorem

Suppose that $\mathbf{N} = \mathbf{Q} \cap \mathcal{K}$ and $\sqrt{Ann(\mathbf{N}/\mathbf{Q})} = \sqrt{Ann(\mathbf{M}/\mathcal{K})}$ for a proper submodule $\mathcal{K}$. Let $\mathbf{Q}_1, \ldots, \mathbf{Q}_r$ be the set of all isolated primary components of $\mathcal{K}$ and set $\mathbf{Q}' = \mathbf{Q} \cap \bigcap_{i=1}^{r} \mathbf{Q}_i$. If $\mathbf{N} = \mathbf{Q}' \cap \mathcal{K}'$ and $\sqrt{Ann(\mathbf{M}/\mathcal{K}')} = \sqrt{Ann(\mathbf{N}/\mathbf{Q}')}$ for a proper submodule $\mathcal{K}'$, then any minimal associated prime of $\mathcal{K}'$ is a non-associated prime of $\mathcal{K}$. In particular any minimal associated prime of $\mathcal{K}'$ properly contains a minimal associated prime of $\mathcal{K}$.

Basic Results

Lemma

- Let $\mathcal{N} \subset \mathbb{Z}[x]^s$ be $\mathbb{Z}[x]$-modules with $\mathrm{Ann}(\mathbb{Z}[x]^s/\mathcal{N}) \cap \mathbb{Z} = \langle 0 \rangle$. Let $\mathcal{N}\mathbb{Q}[x] = \overline{Q}_1 \cap \ldots \cap \overline{Q}_s$ be an irredundant primary decomposition with associated primes $\overline{P}_i = \sqrt{\mathrm{Ann}(\mathbb{Z}[x]^s/\overline{Q}_i)}$, then $\mathcal{N}\mathbb{Q}[x] \cap \mathbb{Z}[x]^s = (\overline{Q}_1 \cap \mathbb{Z}[x]^s) \cap \ldots \cap (\overline{Q}_s \cap \mathbb{Z}[x]^s)$ is an irredundant primary decomposition with associated primes $\overline{P}_i \cap \mathbb{Z}[x] = \sqrt{\mathrm{Ann}(\mathbb{Z}[x]^s/\overline{Q}_i) \cap \mathbb{Z}[x]}$.

Basic Results

Lemma

- Let $\mathcal{N} \subset \mathbb{Z}[x]^s$ be $\mathbb{Z}[x]$-modules with $\mathrm{Ann}(\mathbb{Z}[x]^s/\mathcal{N}) \cap \mathbb{Z} = \langle 0 \rangle$. Let $\mathcal{N}\mathbb{Q}[x] = \overline{Q}_1 \cap \ldots \cap \overline{Q}_s$ be an irredundant primary decomposition with associated primes $\overline{P}_i = \sqrt{\mathrm{Ann}(\mathbb{Z}[x]^s/\overline{Q}_i)}$, then $\mathcal{N}\mathbb{Q}[x] \cap \mathbb{Z}[x]^s = (\overline{Q}_1 \cap \mathbb{Z}[x]^s) \cap \ldots \cap (\overline{Q}_s \cap \mathbb{Z}[x]^s)$ is an irredundant primary decomposition with associated primes $\overline{P}_i \cap \mathbb{Z}[x] = \sqrt{\mathrm{Ann}(\mathbb{Z}[x]^s/\overline{Q}_i) \cap \mathbb{Z}[x]}$.

Lemma

- Let $\mathcal{N} \subset \mathbb{Z}[x]^s$ be $\mathbb{Z}[x]$-modules with $\mathrm{Ann}(\mathbb{Z}[x]^s/\mathcal{N}) \cap \mathbb{Z} = \langle q \rangle$ and $q = p_1^{\nu_1} \cdot \ldots \cdot p_r^{\nu_r}$ be the prime factorization. Then $\mathcal{N} = \bigcap_{i=1}^{r} \langle \mathcal{N} + p_i^{\nu_i} \mathbb{Z}[x]^s \rangle$.

Basic Results

Lemma

- Let $\mathcal{N} \subset \mathbb{Z}[x]^s$ be $\mathbb{Z}[x]$-modules such that $\mathrm{Ann}(\mathbb{Z}[x]^s/\mathcal{N}) \cap \mathbb{Z} = \langle p^\nu \rangle$ for some prime number p . Moreover, let $\mathrm{minAss}(\mathcal{N}\mathbb{F}_p[x]) = \{\overline{P}_1, \ldots, \overline{P}_s\}$ be the set of minimal associated prime ideals of $\mathcal{N}\mathbb{F}_p[x]$ and $P_1, \ldots, P_s$ be the canonical liftings to $\mathbb{Z}[x]$. Then $\mathrm{minAss}(\mathcal{N}) = \{P_1, \ldots, P_s\}$ is the set of minimal associated primes of $\mathcal{N}$.
  If $\nu = 1$ let $\mathcal{N}\mathbb{F}_p[x] = \overline{Q}_1 \cap \ldots \cap \overline{Q}_s$ be an irredundant primary decomposition with associated primes $\overline{P}_1, \ldots, \overline{P}_s$ and $Q_1, \ldots, Q_s$ resp. $P_1, \ldots, P_s$ be the canonical liftings to $\mathbb{Z}[x]^s$ resp. $\mathbb{Z}[x]$. Then $\mathcal{N} = Q_1 \cap \ldots \cap Q_s$ is an irredundant primary decomposition with associated primes $P_1, \ldots, P_s$.

Definition

- An ideal I of $\mathbb{Z}[x]$ is called a pseudo primary ideal if $\sqrt{I}$ is a prime ideal.
- A submodule $\mathcal{N} \subset \mathbb{Z}[x]^s$ is called a pseudo primary submodule of $\mathbb{Z}[x]^s$ if $\mathrm{Ann}(\mathbb{Z}[x]^s/\mathcal{N})$ is a pseudo primary ideal of $\mathbb{Z}[x]$.
- Let $\mathcal{N}$ be a submodule of $\mathbb{Z}[x]^s$ and let $\mathrm{minAss}(\mathcal{N}) = \{P_1, P_2, \ldots, P_r\}$, each finite set S_i which satisfies the condition:

$$S_i \cap P_i = \emptyset \text{ and } S_i \cap P_j \neq \emptyset \text{ for } i \neq j.$$

is called a separator of $\mathcal{N}$ with respect to P_i and the set $\{S_1, S_2, \ldots, S_r\}$ is called a system of separators for $\mathcal{N}$.

Lemma

- Let $\mathcal{N}$ be a submodule of $\mathbb{Z}[x]^s$ over $\mathbb{Z}[x]$ and let S be a multiplicatively closed subset of $\mathbb{Z}[x]$, $t = \prod_{s_i \in S} s_i$, then there exists an integer k such that
$\mathcal{N} : t^k = \mathbb{Z}[x]_t\mathcal{N} \cap \mathbb{Z}[x]^s = \mathbb{Z}[x]_S\mathcal{N} \cap \mathbb{Z}[x]^s$.

Lemma

- Let $\mathcal{N}$ be a submodule of $\mathbb{Z}[x]^s$ over $\mathbb{Z}[x]$ and let S be a multiplicatively closed subset of $\mathbb{Z}[x]$, $t = \prod_{s_i \in S} s_i$, then there exists an integer k such that
  $\mathcal{N} : t^k = \mathbb{Z}[x]_t\mathcal{N} \cap \mathbb{Z}[x]^s = \mathbb{Z}[x]_S\mathcal{N} \cap \mathbb{Z}[x]^s$.

Lemma

- Let $\mathcal{N} \subseteq \mathbb{Z}[x]^s$ be submodules and let $f \in \mathbb{Z}[x]$ such that $\mathcal{N} : f^k = \mathcal{N} : f^{k+1}$ then $\mathcal{N}$ can be splitted as
  $\mathcal{N} = (\mathcal{N} : f^k) \cap (\mathcal{N} + f^k\mathbb{Z}[x]^s)$.

pseudo–primary decomposition

Lemma (T. Shimoyama, K. Yokoyama)

- Let $\mathcal{N}$ be submodules of $\mathbb{Z}[x]^s$. Let $\mathrm{minAss}(\mathcal{N}) = \{P_1, P_2, \ldots, P_r\}$ and $\{S_1, S_2, \ldots, S_r\}$ be a system of separators for $\mathcal{N}$. For each i, let $\overline{Q}_i = \mathbb{Z}[x]_{S_i}\mathcal{N} \cap \mathbb{Z}[x]^s$, let $s_i = \prod_{s \in S_i} s$ and k_i be an integer such that $\mathbb{Z}[x]_{S_i}\mathcal{N} \cap \mathbb{Z}[x]^s = (\mathcal{N} : s_i^{k_i})$, then

$$\mathcal{N} = \overline{Q}_1 \cap \overline{Q}_2 \cap \ldots \cap \overline{Q}_r \cap \mathcal{N}' \quad (*)$$

where $\mathcal{N}' = \mathcal{N} + s_1^{k_1}\mathbb{Z}[x]^s + \ldots + s_r^{k_r}\mathbb{Z}[x]^s$. Moreover, either $\mathcal{N}' = \mathbb{Z}[x]^s$ or $\dim(\mathrm{Ann}(\mathbb{Z}[x]^s/\mathcal{N}')) < \dim(\mathrm{Ann}(\mathbb{Z}[x]^s/\mathcal{N}))$.

pseudo–primary decomposition

Lemma (T. Shimoyama, K. Yokoyama)

- Let $\mathcal{N}$ be submodules of $\mathbb{Z}[x]^s$. Let $\mathrm{minAss}(\mathcal{N}) = \{P_1, P_2, \ldots, P_r\}$ and $\{S_1, S_2, \ldots, S_r\}$ be a system of separators for $\mathcal{N}$. For each i, let $\overline{Q}_i = \mathbb{Z}[x]_{S_i}\mathcal{N} \cap \mathbb{Z}[x]^s$, let $s_i = \prod_{s \in S_i} s$ and k_i be an integer such that $\mathbb{Z}[x]_{S_i}\mathcal{N} \cap \mathbb{Z}[x]^s = (\mathcal{N} : s_i^{k_i})$, then

$$\mathcal{N} = \overline{Q}_1 \cap \overline{Q}_2 \cap \ldots \cap \overline{Q}_r \cap \mathcal{N}' \quad (*)$$

  where $\mathcal{N}' = \mathcal{N} + s_1^{k_1}\mathbb{Z}[x]^s + \ldots + s_r^{k_r}\mathbb{Z}[x]^s$. Moreover, either $\mathcal{N}' = \mathbb{Z}[x]^s$ or $\dim(\mathrm{Ann}(\mathbb{Z}[x]^s/\mathcal{N}')) < \dim(\mathrm{Ann}(\mathbb{Z}[x]^s/\mathcal{N}))$.

- Each $\overline{Q}_i = (\mathcal{N} : s_i^{k_i})$ is called a pseudo primary component of $\mathcal{N}$ and $\mathcal{N}'$ is called the remaining component in the pseudo primary decomposition.

Extraction Lemma

Let $\mathcal{N} = Q \cap J$ be pseudo–primary submodule of $\mathbb{Z}[x]^s$ with $\sqrt{\mathrm{Ann}(\mathbb{Z}[x]^s/Q)} = P$ and Q be P–primary with $\mathrm{ht}(Q) < \mathrm{ht}(J)$. Let $P \cap \mathbb{Z} = \langle p \rangle$ for some prime p and $u \subset x$ be a maximal independent set of variables for $\overline{P} = P\mathbb{F}_p[x]$. Let $A := \mathbb{Z}[u]_{\langle p \rangle}$, then the following holds:

Extraction Lemma

Let $\mathcal{N} = Q \cap J$ be pseudo–primary submodule of $\mathbb{Z}[x]^s$ with $\sqrt{\mathrm{Ann}(\mathbb{Z}[x]^s/Q)} = P$ and Q be P–primary with $\mathrm{ht}(Q) < \mathrm{ht}(J)$. Let $P \cap \mathbb{Z} = \langle p \rangle$ for some prime p and $u \subset x$ be a maximal independent set of variables for $\overline{P} = P\mathbb{F}_p[x]$. Let $A := \mathbb{Z}[u]_{\langle p \rangle}$, then the following holds:

- $\mathcal{N}A[x \setminus u] \cap \mathbb{Z}[x]^s = Q$

Extraction Lemma

Let $\mathcal{N} = Q \cap J$ be pseudo–primary submodule of $\mathbb{Z}[x]^s$ with $\sqrt{\mathrm{Ann}(\mathbb{Z}[x]^s/Q)} = P$ and Q be P–primary with $\mathrm{ht}(Q) < \mathrm{ht}(J)$. Let $P \cap \mathbb{Z} = \langle p \rangle$ for some prime p and $u \subset x$ be a maximal independent set of variables for $\overline{P} = P\mathbb{F}_p[x]$. Let $A := \mathbb{Z}[u]_{\langle p \rangle}$, then the following holds:

- $\mathcal{N}A[x \setminus u] \cap \mathbb{Z}[x]^s = Q$
- Let G be a strong Gröbner basis of $\mathcal{N}$ w.r.t. a block ordering satisfying $x \setminus u \gg u$. Then G is a strong Gröbner basis of $\mathcal{N}A[x \setminus u]$ w.r.t. the induced ordering for the variables $x \setminus u$.

Extraction Lemma

Let $\mathcal{N} = Q \cap J$ be pseudo–primary submodule of $\mathbb{Z}[x]^s$ with $\sqrt{\mathrm{Ann}(\mathbb{Z}[x]^s/Q)} = P$ and Q be P–primary with $\mathrm{ht}(Q) < \mathrm{ht}(J)$. Let $P \cap \mathbb{Z} = \langle p \rangle$ for some prime p and $u \subset x$ be a maximal independent set of variables for $\overline{P} = P\mathbb{F}_p[x]$. Let $A := \mathbb{Z}[u]_{\langle p \rangle}$, then the following holds:

- $\mathcal{N}A[x \setminus u] \cap \mathbb{Z}[x]^s = Q$
- Let G be a strong Gröbner basis of $\mathcal{N}$ w.r.t. a block ordering satisfying $x \setminus u \gg u$. Then G is a strong Gröbner basis of $\mathcal{N}A[x \setminus u]$ w.r.t. the induced ordering for the variables $x \setminus u$.
- Let $G = \{g_1, \ldots, g_k\}$ be as in (2), $\mathrm{LT}_{A[x \setminus u]}(g_i) = p^{\nu_i} a_i (x \setminus u)^{\beta_i} e_j$ with $a_i \in \mathbb{Z}[u] \setminus \langle p \rangle$ for $i = 1, \ldots, k$, and $h = \mathrm{lcm}(a_1, \ldots, a_k)$. Then $\mathcal{N}A[x \setminus u] \cap \mathbb{Z}[x]^s = \mathcal{N} : h^\infty$.

Extraction Lemma

Let $\mathcal{N} = Q \cap J$ be pseudo–primary submodule of $\mathbb{Z}[x]^s$ with $\sqrt{\mathrm{Ann}(\mathbb{Z}[x]^s/Q)} = P$ and Q be P–primary with $\mathrm{ht}(Q) < \mathrm{ht}(J)$. Let $P \cap \mathbb{Z} = \langle p \rangle$ for some prime p and $u \subset x$ be a maximal independent set of variables for $\overline{P} = P\mathbb{F}_p[x]$. Let $A := \mathbb{Z}[u]_{\langle p \rangle}$, then the following holds:

- $\mathcal{N}A[x \setminus u] \cap \mathbb{Z}[x]^s = Q$
- Let G be a strong Gröbner basis of $\mathcal{N}$ w.r.t. a block ordering satisfying $x \setminus u \gg u$. Then G is a strong Gröbner basis of $\mathcal{N}A[x \setminus u]$ w.r.t. the induced ordering for the variables $x \setminus u$.
- Let $G = \{g_1, \ldots, g_k\}$ be as in (2), $\mathrm{LT}_{A[x \setminus u]}(g_i) = p^{\nu_i} a_i (x \setminus u)^{\beta_i} e_j$ with $a_i \in \mathbb{Z}[u] \setminus \langle p \rangle$ for $i = 1, \ldots, k$, and $h = \mathrm{lcm}(a_1, \ldots, a_k)$. Then $\mathcal{N}A[x \setminus u] \cap \mathbb{Z}[x]^s = \mathcal{N} : h^\infty$.
- $u \subset x$ is called a maximal independent set of variable for $\overline{P} \subset \mathbb{F}_p[x]$ if $\overline{P} \cap \mathbb{F}_p[u] =< 0 >$ and $\sharp u = \dim(\mathbb{F}_p[x]/\overline{P})$

separatorsZ

nput B a list of prime ideals generated by a Gröbner basis w.r.t. some ordering, not contained in each other, $P \in B$.

tput Polynomial s such that $s \notin P$, $s \in Q$ for all $Q \in B \backslash \{P\}$.

- for $(Q \in B \backslash \{P\})$
  choose s_Q in the Gröbner basis of Q such that $s_Q \notin P$;
- return$(\prod_{Q \in B \backslash \{P\}} s_Q)$;

extractZ

nput $\mathcal{N} \subseteq \mathbb{Z}[x]^s$ a submodule, B the list of minimal associated primes of $\mathcal{N}$, $P \in B$ with $P \cap \mathbb{Z} = \langle p \rangle$ for some prime p, $u \subset x$ an independent set of variables for $P\mathbb{F}_p[x]$.

tput The primary component Q of $\mathcal{N}$ associated to P.

- $s :=$ SEPERATORSZ(P, B);
- $\mathcal{N} = \mathcal{N} : s^\infty$;
- compute $G = \{g_1, \ldots, g_k\}$, a strong Gröbner basis of $\mathcal{N}$ w.r.t. a block ordering satisfying $x \setminus u \gg u$;
- compute $\{a_1, \ldots, a_k\}$ such that $LC_{\mathbb{Z}[u]_{\langle p \rangle}[x \setminus u]}(g_i) = p^{\nu_i} \cdot a_i$ with $a_i \in \mathbb{Z}[u] \setminus \langle p \rangle$;
- compute $h = lcm(a_1, \ldots, a_k)$, the least common multiple of $a_1, \ldots, a_k$;
- return $(\mathcal{N} : h^\infty)$;

primdecZ

nput $F_{\mathcal{N}} = \{f_1, \ldots, f_k\}$, $\mathcal{N} = \langle F_{\mathcal{N}} \rangle_{\mathbb{Z}[x]}$, optional: a test ideal T.

tput $L := \{(Q_1, P_1), \ldots, (Q_s, P_s)\}$, $\mathcal{N} = Q_1 \cap \ldots \cap Q_s$ irredundant primary decomposition with $P_i = \sqrt{Q_i}$.

- $\mathrm{Ann}(\mathbb{Z}[x]^s/\mathcal{N}) \cap \mathbb{Z}$=$\langle q \rangle$;
- if $(q = 0)$
- compute $h \in \mathbb{Z}$ such that $\mathcal{N} : h = \mathcal{N}\mathbb{Q}[x] \cap \mathbb{Z}[x]^s$;
- compute $\overline{Q}_1, \ldots, \overline{Q}_s$, an irredundant primary decomposition of $\mathcal{N}\mathbb{Q}[x]$ and $\overline{P}_i = \sqrt{\overline{Q}_i}$ the associated primes;
- compute $Q_i = \overline{Q}_i \cap \mathbb{Z}[x]^s$, $P_i = \overline{P}_i \cap \mathbb{Z}[x]$;

primdecZ

- compute $q = p_1^{\nu_1} \dots p_r^{\nu_r}$, the prime factorization of q;
- if $(\nu_i = 1)$
- compute $\overline{L}_i = \{(\overline{Q}_1^{(i)}, \overline{P}_1^{(i)}), \dots, (\overline{Q}_{s_i}^{(i)}, \overline{P}_{s_i}^{(i)})\}$, the primary decomposition of $\mathcal{N}\mathbb{F}_{p_i}[x]$;
- $L_i := \{(Q_1^{(i)}, P_1^{(i)}), \dots, (Q_{s_i}^{(i)}, P_{s_i}^{(i)})\}$, the lifting of $\overline{L}_i$ to $\mathbb{Z}[x]$;
- else
- compute $\overline{A}_i = \{\overline{P}_1^{(i)}, \dots, \overline{P}_{s_i}^{(i)}\}$, the set of minimal associated primes of $\mathcal{N}\mathbb{F}_{p_i}[x]$ and compute pseudo–primary submodule using Shimoyama–Yokoyama and apply extractZ to extract primary submodules from pseudo–primary submodules.

THANK YOU