Dissertation

Double Ideal Quotient and Effective Localization

Yuki Ishihara
Department of Mathematics
Graduate School of Science
Rikkyo University

2020

Contents

Introduction

"Computer Algebra" is an interdisciplinary field of mathematics and computer science. It mainly concerns algebraic computations over the integer ring, the rational field, finite fields, polynomial rings and so on. Computational aspects of Computer Algebra give us variants of application for pure mathematics and applied mathematics by its symbolic computations. Also, it has developed new areas in mathematics, for example, Gröbner basis, which is a fundamental tool of aspects in computational commutative algebra and algebraic geometry nowadays.

This thesis is mainly dedicated to devise efficient methods for operations in polynomial rings, especially *effective localization of ideals* (at a prime ideal), which also means *direct computation* (extraction) of primary component here. It is well-known that such localization can be computed through "primary decomposition", which is some generalization of factorization of a polynomial. Algorithms of primary decomposition have been much studied, for example, in [10, 12, 19, 26]. However, primary decomposition computes unnecessary primary components for the localization. Thus, we provide new algorithms which obtain the particular primary components directly by using Double Ideal Quotient (DIQ) and its variants. We call such algorithms "Local Primary Algorithms (LPAs)", which is introduced in Chapter 4. To make LPAs more efficiently, we apply modular techniques to computations of ideal quotients in Chapter 5.

Here, we give some details of our approaches. We can consider $\mathrm{hull}(I + P^m)$ as a candidate of a P-primary component of a given ideal I, where P is a prime divisor of I, m is some positive integer, and $\mathrm{hull}(I + P^m)$ is *the equidimensional hull* of $I + P^m$. If m is sufficiently large, $\mathrm{hull}(I + P^m)$ is a P-primary component of I with respect to P. However, we have to check whether m is enough large or not. We invent criteria for primary components by using DIQ and its variants. DIQ of ideals I and J is $(I : (I : J))$ and its variants are $(I : (I : J^\infty))$, $(I : (I : J^\infty)^\infty)$ and $(I : (I : J)^\infty)$. By $(I : (I : J)^\infty)$, we can check whether $\mathrm{hull}(I + P^m)$ is a primary component of I or not. Also, we can use DIQ to compute the equidimensional hull. Based on these criteria, we compose LPAs, by which we can compute the particular primary component without full primary decomposition. In more details, we explain some key points of LPA in the following.

- LPAs are based on several generating tools and criteria for primary components with different procedures for two cases; isolated and embedded.
- LPAs use DIQ and its variants as tools for generating and checking primary components.
- DIQ has already appeared in [28] to check associated primes or compute equidimensional hulls, and in [10], to compute equidimensional radicals. We investigate DIQ and its variants more deeply.
- There are other important properties of DIQ and its variants toward effective localization.

For instance, for ideals I, J and a primary decomposition $\mathcal{Q}$ of I, $(I : (I : J)^{\infty})$ (a variant of DIQ) coincides with $\bigcap_{Q \in \mathcal{Q}, J \subset IK[X]_{\sqrt{Q}} \cap K[X]} Q$.

For practical implementations we devise several efficient techniques for improving our LPAs as follows (see [13, 28] for efficient computation of ideal quotient and saturation).

- ($P_G^{[m]}$-products) Use $P_G^{[m]} = \langle f_1^m, \ldots, f_r^m \rangle$ for some generator $G = \{f_1, \ldots, f_r\}$ of P and the *equidimensional hull* (see Definition 1.1.25) $\mathrm{hull}(I + P_G^{[m]})$ to compute a P-primary component, instead of using $\mathrm{hull}(I + P^m)$ (see Lemma 4.2.3).
- (MIS-hull) Use *a maximal independent set (MIS)* of P for computing $\mathrm{hull}(\overline{Q})$ where $\overline{Q}$ is a P-hull-primary ideal (see Definition 1.1.29 for MIS and Definition 1.3.1 for hull-primary). Since an MIS U of P is also an MIS of $I + P^m$, we obtain that $\mathrm{hull}(I + P^m) = (I + P^m)K[X]_{K[U]^{\times}} \cap K[X]$ (see Lemma 4.2.7).
- (MIS-localization) Use an MIS U of P at the first step of LPA to replace I for $IK[X]_{K[U]^{\times}} \cap K[X]$ (see Theorem 3.2.7).

Thanks to efficient techniques above, our experiment shows clearly the practicality of our direct localization method. From our experiments, we conclude that MIS-localization is the most efficient among techniques for LPAs. However, there are some cases for which it is not efficient. Our main observation is the following;

- LPAs have strong effectiveness by its speciality.
- MIS-localization is much effective for many examples (see Table 6.1 in Chapter 6). However, its computational behavior is *unstable* (see Figures 6.2, 6.3 in Chapter 6).
- Effectiveness of LPAs depends on ideals. At present, it is not predicable and thus it would be better to apply them in parallel.

Next, we explain modular techniques for (double) ideal quotient and saturation. LPAs compute the specific primary component from given a prime ideal without full primary decomposition. However, they tend to be very time-consuming for their computations of Gröbner bases and ideal quotients in some cases. Also, there is another problem; we have to find candidates of prime divisors. To solve these problems, we provide a new method for computing DIQ in the n variables polynomial ring with rational coefficients $\mathbb{Q}[X] = \mathbb{Q}[x_1, \ldots, x_n]$ by using "modular techniques". It is well-known that modular techniques are useful to avoid *intermediate coefficient growth* and have a good relationship with parallel computing (see [2, 7, 14, 23]). We apply modular techniques as follows.

(1) Apply modular techniques to DIQ. (Theorem 5.2.8 and Theorem 5.2.9)

(2) Extend criteria about prime divisor and primary component presented in Chapter 3. (Theorem 5.1.3 and Theorem 5.1.6)

(3) Devise a new method for certain intermediate decomposition in some special cases. (Corollary 5.3.2 and Proposition 5.3.4)

By the effectiveness of modular techniques, we can compute ideal quotients and saturations much faster in our computer experiments. Here, we describe details of modular techniques. For a prime number p, let $\mathbb{Z}_{(p)} = \{a/b \in \mathbb{Q} \mid a, b \in \mathbb{Z} \text{ and } p \nmid b\}$ be the localized ring by p and $\mathbb{F}_p[X]$ the polynomial ring over the finite field of order p. We denote by ϕ_p the canonical projection $\mathbb{Z}_{(p)}[X] \to \mathbb{F}_p[X]$. As an example, we see modular techniques for DIQ. Given ideals I and J in the polynomial ring with rational coefficients $\mathbb{Q}[X]$, we first compute DIQ of the image $\phi_p((I : (I : J)) \cap \mathbb{Z}_{(p)}[X])$ in $\mathbb{F}_p[X]$ for "lucky" primes p (we will discuss such luckiness in Definition 5.2.1). Next, we lift them up to G_{can}, a candidate of Gröbner basis, from the computed Gröbner basis $\bar{G}$ of $\phi_p((I : (I : J)) \cap \mathbb{Z}_{(p)}[X])$ by using Chinese Remainder Theorem (CRT) and rational reconstruction (see [7]). Avoiding intermediate coefficient growth, this method is efficient for several examples.

For finding prime divisors, we provide certain "intermediate decomposition" of ideals by extending the criterion presented in Chapter 3 about prime divisors. For an ideal I and a prime ideal P, it follows that P is a prime divisor of I if and only if $P \supset (I : (I : P))$ (see Theorem 3.3.1). However, the projected image of a prime ideal may not be a prime ideal but an intersection of prime ideals in $\mathbb{F}_p[X]$. Thus, we generalize the criterion to a radical ideal $J \supset I$; it follows that every prime divisor P of J is associated with I if and only if $J \supset (I : (I : J))$. For such a radical ideal J, if J is unmixed, we can compute the intersection of primary components Q of I whose associated prime is a prime divisor of J by modular techniques. This ideal may be considered as an "intermediate component" of I. By gathering these intermediate components, we may obtain an "intermediate primary decomposition" (see Definition 5.3.1). For this computation, we can utilize MISs.

This thesis is organized as follows. Throughout the thesis, we omit proofs of well-known theorems and lemmas but include proofs of results appearing in the author's papers ([15, 17, 18]). In Chapter 1, we provide mathematical basis for our criteria and algorithms. In Chapter 2, we introduce notions and properties of DIQ and its variants. In Chapter 3, we describe criteria for prime divisors and primary components by using DIQ and its variants. In Chapter 4, we explain LPAs to compute the particular primary component without primary decomposition, after isolated and embedded prime divisor checks. Also, we generalize propositions in Chapter 3 and devise another algorithm using the splitting tool and MIS instead of DIQ to compare it and LPAs. In Chapter 5, we invent modular techniques for (double) ideal quotient and saturation. In Chapter 6, we tested for many examples as experiments and discuss the behavior of each algorithm. Finally, we give some concluding remarks and the future works. The work of LPAs is based on [17] and [18], and that of modular techniques for localization is based on [15].

Acknowledgements

First of all, the author would like to express his grateful for his supervisor Professor Kazuhiro Yokoyama. Without his kind supports and helpful advice, the author could not complete his thesis and stand up at the first step of his research life. Also, he would like to appreciate that the dissertation committee reviewed this thesis and gave him helpful comments and suggestions. The work about modular techniques has been advanced during the author's research stay at Technische Universität Kaiserslautern, supported by Overseas Challenge Program for Young Researchers of Japan Society for the Promotion of Science. The author is very grateful to the SINGULAR team for fruitful discussions and kind hospitality there. In particular, he is very thankful to Professor Wolfram Decker and Dr. Hans Schönemann for helpful advice of modular techniques and programming on SINGULAR at Kaiserslautern. He appreciates the kind support of the computational facility by Professor Masayuki Noro. The author would like to thank all people who helped his life, for example,

his friends and his family. The author is thankful to Dr. Tristan Vaccon for his hospitality during the short stay at Limoges. Also, he expresses his grateful for Dr. Ryoya Fukasaku, whose thesis is very helpful for writing this thesis. He thanks his best friends Nobukatsu Watanabe, Shunsuke Kurima, Yuta Kambe, and Keitaro Kitagawa for their very warm friendships. Finally, he dedicate this thesis to his parents Hatsumi Ishihara and Heikichi Ishihara.

Chapter 1

Mathematical Basis

Throughout this thesis, we let K be a computable field (e.g. the rational field $\mathbb{Q}$ or a finite field $\mathbb{F}_p$) of order p, $X = \{x_1, \ldots, x_n\}$ a set of variables and $K[X] = K[x_1, \ldots, x_n]$ the polynomial ring over K. We write $\langle f_1, \ldots, f_t \rangle_{K[X]}$ for the ideal generated by elements $f_1, \ldots, f_t$ in $K[X]$ and we simply use $\langle f_1, \ldots, f_t \rangle$ if the ring is obvious. When we simply say that I is an ideal, it means the I is a proper ideal of $K[X]$. Moreover, we denote the radical $\{f \in K[X] \mid f^m \in I \text{ for some } m \in \mathbb{Z}_{\geq 0}\}$ of I by $\sqrt{I}$.

1.1 Fundamental Definitions

First, we introduce a definition of *Gröbner basis*, which is a basic tool in Computer Algebra. Gröbner basis is defined with respect to each *monomial ordering*. Here, we write $X^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ for $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n$.

Definition 1.1.1 (Monomial Ordering; [13], Definition 1.2.1 and Definition 1.2.4)**.** A monomial ordering (a global ordering) $\prec$ *on* $K[x_1, \ldots, x_n]$ *is a relation on the set of monomials* X^α, $\alpha \in \mathbb{Z}_{\geq 0}^n$, *satisfying:*

(1) $\prec$ *is a total ordering on* $\{X^\alpha \mid \alpha \in \mathbb{Z}_{\geq 0}^n\}$.

(2) If $X^\alpha \prec X^\beta$ *and* $\gamma \in \mathbb{Z}_{\geq 0}^n$, *then* $X^{\alpha+\gamma} \prec X^{\beta+\gamma}$.

(3) $1 \prec X^\alpha$ *for all* $\alpha \in \mathbb{Z}_{\geq 0}^n$.

To compute Gröbner basis efficiently, we often use the graded reverse lexicographic ordering as follows.

Example 1.1.2 (Graded Reverse Lexicographic Ordering (Degree Reverse Lexicographic Ordering); [8], Chapter 2, Section 2, Definition 6)**.** *Let* $\alpha = (\alpha_1, \ldots, \alpha_n), \beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}_{\geq 0}^n$. *We say that* $X^\alpha \succ_{grevlex} X^\beta$ *if*

$$|\alpha| > |\beta| \text{ or } |\alpha| = |\beta| \text{ and the rightmost nonzero entry of } \alpha - \beta \text{ is negative,}$$

where $|\alpha| = \alpha_1 + \cdots + \alpha_n$ *and* $|\beta| = \beta_1 + \cdots + \beta_n$.

Remark 1.1.3 (Block Ordering; [13], p.14)**.** *Let $\prec_1$ and $\prec_2$ be monomial orderings on $K[X] = K[x_1, \ldots, x_n]$ and $K[Y] = K[y_1, \ldots, y_m]$ respectively. Then the product ordering or block ordering $\prec = (\prec_1, \prec_2)$ on $K[X, Y] = K[x_1, \ldots, x_n, y_1, \ldots, y_m]$ is defined as*

$$X^\alpha Y^\beta \succ X^{\alpha'} Y^{\beta'} \Longleftrightarrow X^\alpha \succ_1 X^{\alpha'} \text{ or } (X^\alpha = X^{\alpha'} \text{ and } Y^\beta \succ_2 Y^{\beta'}).$$

Here, if $\prec_1$ and $\prec_2$ are irrelevant, we write just $X \succ\succ Y$.

We consider the leading term of a polynomial with respect to each monomial ordering. Here, we also consider an ordering on $\mathbb{Z}^n_{\geq 0}$ coming from $\prec$ and write $\alpha \prec \beta$ if $X^\alpha \prec X^\beta$.

Definition 1.1.4 (Initial Terms; [8], Chapter 2, Section 2, Definition 7)**.** *Let $f = \sum_\alpha a_\alpha X^\alpha$ be a nonzero polynomial in $K[X] = K[x_1, \ldots x_n]$ and let $\prec$ be a monomial ordering.*

(1) The multidegree *of f is* $\mathrm{multideg}(f) = \max_\prec\{\alpha \in \mathbb{Z}^n_{\geq 0} \mid a_\alpha \neq 0\}$.

(2) The initial coefficient *of f is* $\mathrm{lc}_\prec(f) = a_{\mathrm{multideg}(f)} \in K$.

(3) The initial monomial *(or power product) of f is* $\mathrm{lp}_\prec(f) = X^{\mathrm{multideg}(f)}$.

(4) The initial term *of f is* $\mathrm{lt}_\prec(f) = \mathrm{lc}_\prec(f)\mathrm{lp}_\prec(f)$.

Letting $\mathrm{lt}_\prec(I) = \{\mathrm{lt}_\prec(f) \mid 0 \neq f \in I\}$, we call $\langle \mathrm{lt}_\prec(I)\rangle$ the initial ideal of I. If $\prec$ is obvious, we simply write $\mathrm{lc}(f)$, $\mathrm{lp}(f)$ and $\mathrm{lt}(f)$.

Example 1.1.5. *Let $\prec$ be the graded reverse lexicographic ordering (or the degree reverse lexicographic ordering) with $x \succ y \succ z$ and $f = 3xy^2z + 2x^2yz + z^3$. Then,*

$$\begin{aligned} \mathrm{multideg}(f) &= (2, 1, 1), \\ \mathrm{lc}_\prec(f) &= 2, \\ \mathrm{lp}_\prec(f) &= x^2yz, \\ \mathrm{lt}_\prec(f) &= 2x^2yz. \end{aligned}$$

Here, we define a *Gröbner basis* of an ideal to compute various ideal operations. It was introduced by Bruno Buchberger in his Ph.D thesis ([6]).

Definition 1.1.6 (Gröbner basis; [8], Chapter 2, Section 5, Definition 5 and Chapter 2, Section 7, Definition 4)**.** *Let $\prec$ be a monomial ordering and I an ideal in $K[X]$. A finite subset $G = \{g_1, \ldots g_r\} \neq \{0\}$ of I is called a* Gröbner basis *of I with respect to $\prec$ if*

$$\langle \mathrm{lt}_\prec(g_1), \ldots, \mathrm{lt}_\prec(g_r)\rangle = \langle \mathrm{lt}_\prec(I)\rangle.$$

Moreover, G is called the reduced Gröbner basis *of I with respect to $\prec$ if G is a Gröbner basis of I with respect to $\prec$ and*

(1) $\mathrm{lc}_\prec(g_i) = 1$ for all i.

(2) For all i, no monomial of g_i lies in $\langle \mathrm{lt}_\prec(G \setminus \{g_i\})\rangle$.

Example 1.1.7. *Let $I = \langle x^2 + xy + z^2, xz + yz + z^2\rangle \subset \mathbb{Q}[x, y, z]$. Then, $G = \{x^2 + xy + z^2, xz + yz + z^2, yz^2 + 2z^3\}$ is the reduced Gröbner basis of I with respect to $\succ_{grevlex}$ with $x \succ y \succ z$.*

We introduce the notions of S-polynomial and a remainder on division for a criterion of Gröbner basis.

Definition 1.1.8 ([8], Chapter 2, Section 6, Definition 4)**.** *Let $f, g \in K[X]$ be nonzero polynomials with* multideg$(f) = \alpha$ *and* multideg$(g) = \beta$*. Let $\gamma = (\gamma_1, \ldots, \gamma_n)$, where $\gamma_i = \max\{\alpha_i, \beta_i\}$ for each i (i.e. $X^\gamma = \mathrm{lcm}(X^\alpha, X^\beta)$). Then, the* S-polynomial *of f and g is the combination*

$$S(f,g) = \frac{X^\gamma}{\mathrm{lt}(f)} f - \frac{X^\gamma}{\mathrm{lt}(g)} g.$$

Definition 1.1.9 (Division Algorithm; [8], Chapter 2, Section 3, Theorem 3)**.** *Let $\prec$ be a monomial ordering and $F = (f_1, \ldots, f_s)$ be an ordered s-tuple of polynomials in $K[X]$. Then, every $f \in K[X]$ can be written as*

$$f = q_1 f_1 + \cdots + q_s f_s + r,$$

where $q_i, r \in K[X]$, and either $r = 0$ or r is a linear combination, with coefficients in K, of monomials, none of which is divisible by any $\mathrm{lt}(f_1), \ldots, \mathrm{lt}(f_s)$*. Furthermore, if $q_i f_i \neq 0$, then* multideg$(f) \geq$ multideg$(q_i f_i)$*. We call r a* remainder *of f on division F and denote it by* $\mathrm{rem}_F(f)$*.*

We can check if a given generating set is Gröbner basis or not by the following famous criterion.

Theorem 1.1.10 (Buchberger's Criterion; [8], Chapter 2, Section 6, Theorem 6)**.** *Let I be an ideal. Then a generating set $G = \{g_1, \ldots, g_r\}$ of I is a Gröbner basis of I if and only if for all pairs $i \neq j$, the remainder on division of $S(g_i, g_j)$ by G (listed in some order) is zero.*

Also, we can compute a Gröbner basis of a given ideal by using Buchberger's Criterion.

Buchberger's algorithm; [8], Chapter 2, Section 7, Theorem 2

Input: $F = \{f_1, \ldots, f_r\}$: a generating set of an ideal I in $\mathbb{Q}[X]$ and $\prec$: a monomial ordering.
Output: a Gröbner basis G of I with respect to $\prec$.

$G \leftarrow F$.
$G' \leftarrow \{\}$
WHILE $G' \neq G$
    $G' \leftarrow G$
    FOR each pair $(p, q) \in G \times G$ with $p \neq q$,
        $r_{(p,q)} \leftarrow \mathrm{rem}_{G'}(S(p, q))$
        IF $r_{(p,q)} \neq 0$, THEN $G \leftarrow G \cup \{r_{(p,q)}\}$
RETURN G

Next, we introduce the ideal quotient and the saturation of a pair of two ideals (see Section 1.4 for computations). These computations are very important for our LPAs.

Definition 1.1.11 (Ideal Quotient, Saturation; [8], Chapter 4, Section 4, Definitions 5 and 8)**.** *Let I and J be ideals in $K[X]$. Then the ideal*

$$\{f \in K[X] \mid fg \in I \text{ for all } g \in J\}$$

is called the ideal quotient *of I by J and denoted by $(I : J)$. Also, the ideal*

$$\{f \in K[X] \mid \textit{for all } g \in J, \textit{ there is } m \geq 0 \textit{ s.t. } fg^m \in I\}$$

is called saturation *of I with respect to J and denoted by $(I : J^\infty)$.*

Example 1.1.12. *Let $I = \langle x^3, xy\rangle = \langle x\rangle \cap \langle x^3, y\rangle$ and $J = \langle x, y\rangle$ in $\mathbb{Q}[x, y]$. Then, $(I : J) = \langle x^2, xy\rangle = \langle x\rangle \cap \langle x^2, y\rangle$ and $(I : J^\infty) = \langle x\rangle$.*

Remark 1.1.13. *For ideals I, J, and H, $(I \cap J : H) = (I : H) \cap (J : H)$ (see Exercise 1.12 in [1])*

Here we refer the definitions of *prime ideal*, *(P-)primary ideal* and *primary decomposition* to several books [1, 13, 28].

Definition 1.1.14 (Primary Decomposition; [26], Definition 2.1)**.** *For an ideal I of $K[X]$, a set $\mathcal{Q}$ of primary ideals is called* a general primary decomposition *of I if $I = \bigcap_{Q\in\mathcal{Q}} Q$. A general primary decomposition $\mathcal{Q} = \{Q_1, \ldots, Q_r\}$ is a primary decomposition (or irredundant) if the $\sqrt{Q_i}$ are all distinct and $Q_i \not\supset \bigcap_{j\neq i} Q_j$. For a primary decomposition of I, each primary ideal is called* a primary component *of I. The prime ideal associated with a primary component of I is called* a prime divisor *of I. The set of prime divisors is determined independently from the choice of primary decompositions. A primary component Q is called a P-primary component for $P = \sqrt{Q}$. Among all prime divisors of I, minimal prime ideals are called* isolated prime divisors *of I and others are called* embedded prime divisors *of I. A primary component of I is called* isolated *if its prime divisor is isolated and* embedded *if its prime divisor is embedded. We denote by* $\mathrm{Ass}(I)$ *and* $\mathrm{Ass}_{iso}(I)$ *the set of all prime divisors of I and the set of all isolated prime divisors respectively.*

It is well-known that an isolated primary component does not depend on primary decompositions, while an embedded primary component does. From an algorithmic point of view, computation of embedded primary components tends to be more difficult than that of isolated primary components.

We also give fundamental notions and properties related to *localization* that can extract the particular primary components.

Definition 1.1.15 (Multiplicatively Closed Set; [13], Definition 1.4.4)**.** *A subset S of $K[X]$ is called a multiplicatively closed set if*

(1) $1 \in S$,

(2) $ab \in S$ *for all* $a, b \in S$.

Definition 1.1.16 (Localization; [26], Definition 2.2)**.** *Let I be an ideal and S a multiplicatively closed set in $K[X]$. Here, we assume that a multiplicatively closed set always does not contain* 0*. We call $\{f/s \mid f \in I, s \in S\} \subset K(X)$* the localized ideal with respect to *S and denote it by $IK[X]_S$. Also, we call $IK[X]_S \cap K[X]$* the contraction of the localized ideal*. For simplicity, we call the latter the* localization of *I with respect to S (see Definition 2.2 in [26]). For a multiplicatively closed set $K[X] \setminus P$, where P is a prime ideal, we denote it simply by $IK[X]_P \cap K[X]$ and call it the localization of I at P. Also, we write $I_P = IK[X]_P \cap K[X]$ when there is no confusion.*

Example 1.1.17. *In $\mathbb{Q}[X] = \mathbb{Q}[x, y]$, let $P = \langle x\rangle$ be a prime ideal. For $S = \mathbb{Q}[X] \setminus P$ and $I = \langle x^2, xy\rangle$, the localization of I with respect to S is $I\mathbb{Q}[X]_S \cap \mathbb{Q}[X] = \langle x\rangle$. For $P = \langle x, y\rangle$ and $J = \langle x\rangle \cap \langle x + 1\rangle \cap (x + 2, y^2)$, the localization of J at P is $J\mathbb{Q}[X]_P \cap \mathbb{Q}[X] = \langle x\rangle$.*

We remark a relationship between primary decomposition and localization.

Remark 1.1.18 (Localization from Primary Decomposition)**.** *Given a primary decomposition $\mathcal{Q}$ of an ideal I, the localization of I with respect to S can be expressed as $\bigcap_{Q\in\mathcal{Q},Q\cap S=\emptyset} Q$. Moreover, it is also equal to $(I : (\bigcap_{P\in \mathrm{Ass}(I),P\cap S\neq\emptyset} P)^{\infty})$. Here, we are thinking mainly about* computable *multiplicatively closed set s.t. finitely generated one or the complement of a prime ideal. In these cases, we can decide efficiently whether Q and S intersect or not, by using Gröbner basis. Thus if we know all primary components or all associated primes, then we can compute localizations of I for any* computable *multiplicatively closed sets S. However, this method is not a direct method since it computes unnecessary primary components or associated primes.*

Next we introduce the notion of pseudo-primary ideal, which is an extension of that of primary ideal.

Definition 1.1.19 ([26], Definition 2.3)**.** *Let Q be an ideal. We say that Q is* pseudo-primary *if $\sqrt{Q}$ is a prime ideal. In this case, we also say that Q is $\sqrt{Q}$-*pseudo-primary.

Example 1.1.20. *Since $\sqrt{\langle x^2, xy\rangle} = \langle x\rangle$ is a prime ideal, it follows that $\langle x^2, xy\rangle$ is an $\langle x\rangle$-pseudo-primary ideal. Every P-primary ideal is P-pseudo-primary.*

With the notion of pseudo-primary ideal, we can define some special localization *P-pseudo-primary component* with respect to its isolated prime divisor P. The minimal P-pseudo-primary component is equal to the intersection of all primary components whose radicals contain P but do not contain other isolated prime divisors. Here, for a finite set S, we denote by $\langle\langle S\rangle\rangle$ the multiplicatively closed set generated by S.

Definition 1.1.21 (Pseudo-primary component; [26], Definition 2.5)**.** *Let I be an ideal, which is not a pseudo-primary ideal, $P_1, \ldots, P_r$ all isolated prime divisors of I, and $S_1, \ldots, S_r$ are finite subsets in $K[X]$. Each S_i is called a* separator *of I with respect to P_i if they satisfy the following conditions;*

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

A set of separators $\{S_1, \ldots, S_r\}$ is called a system of separators *of I. For a separator S_i of I with respect to P_i, $IK[X]_{\langle\langle S_i\rangle\rangle} \cap K[X]$ is called a P-*pseudo-primary component *of I.*

We can consider the *minimal* pseudo-primary component of I as follows.

Proposition 1.1.22. *Let I be an ideal and P an isolated prime divisor of I. For a set of prime divisors*

$$A(P) = \{P' \in \mathrm{Ass}(I) \mid P' \text{contains } P \text{ but not any other isolated prime divisors of } I\}$$

and the multiplicatively closed set $S = K[X] \setminus \bigcup_{P'\in A(P)} P'$, it follows that $\overline{Q} = IK[X]_S \cap K[X]$ is a pseudo-primary component of I with respect to P. Moreover, $\overline{Q}$ is minimal *among all P-pseudo-primary components with respect to any systems of separators of I.*

Proof. First, we show that $\overline{Q} = IK[X]_S \cap K[X]$ is a pseudo-primary component of I with respect to P. Let $\mathrm{Ass}_{iso}(I) = \{P_1, \ldots, P_r\}$ with $P_1 = P$. Since $P_j \setminus \bigcup_{P'\in A(P_i)} P'$ is not empty for $i \neq j$ from the Prime Avoidance Lemma (see Lemma 1.2.9), there is $s_{ij} \in P_j \setminus \bigcup_{P'\in A(P_i)} P'$. Then $S_i = \{s_{ij} \mid j \neq i\}$ is a separator of I with respect to P_i. Indeed, S_i satisfies $S_i \cap P_i = \emptyset$ and $s_{ij} \in S_i \cap P_j \neq \emptyset$ for $i \neq j$.

For $P' \in \mathrm{Ass}(I)$, if $P' \cap S_1 = \emptyset$, then $P' \in A(P_1)$; otherwise, $s_{1j} \in P' \cap S_1$ for some j. Conversely, if $P' \in A(P_1)$ then $P' \cap S_1 = \emptyset$ by the definition of S_1. Thus, for $P' \in \mathrm{Ass}(I)$, $P' \cap S_1 = \emptyset$ if and only if $P' \in A(P_1)$. Hence, $IK[X]_S \cap K[X] = IK[X]_{\langle\langle S_1\rangle\rangle} \cap K[X]$ and it is a pseudo-primary component of I with respect to P.

Next, we prove the minimality of $IK[X]_S \cap K[X]$. Let $\{S'_1, \ldots, S'_r\}$ be another system of separators of I, where S'_i is a separator with respect to P_i. Also, let $\mathcal{Q}$ be a primary decomposition of I. It is enough to show that $IK[X]_S \cap K[X] = \bigcap_{Q' \in \mathcal{Q}, \sqrt{Q'} \in A(P)} Q' \subset IK[X]_{\langle\langle S'_1\rangle\rangle} \cap K[X]$. Let $Q' \in \mathcal{Q}$ such that $Q' \cap \langle\langle S'_1\rangle\rangle = \emptyset$ (i.e. $\sqrt{Q'} \cap \langle\langle S'_1\rangle\rangle = \emptyset$). Here, we consider an isolated prime divisor P'' contained in $\sqrt{Q'}$. Then $P'' \cap S'_1 = \emptyset$ from $\sqrt{Q'} \cap \langle\langle S'_1\rangle\rangle = \emptyset$. Since $P_j \cap S'_1 \neq \emptyset$ for $j \neq 1$, we obtain that $P'' = P_1$. Thus $\sqrt{Q'}$ contains P_1 but not any other isolated prime divisors i.e. $\sqrt{Q'} \in A(P_1)$. Hence, $IK[X]_S \cap K[X] = \bigcap_{Q' \in \mathcal{Q}, \sqrt{Q'} \in A(P_1)} Q' \subset \bigcap_{Q' \in \mathcal{Q}, Q' \cap \langle\langle S'_1\rangle\rangle = \emptyset} Q' = IK[X]_{\langle\langle S'_1\rangle\rangle} \cap K[X]$. □

Remark 1.1.23. *Every P-pseudo-primary component of I is a P-pseudo-primary ideal. Let $\overline{Q}_P$ be the minimal P-pseudo-primary component of I. Then $I = \bigcap_{P \in \mathrm{Ass}_{iso}(I)} \overline{Q}_P \cap I'$ for some I' s.t. $\mathrm{Ass}_{iso}(I') \cap \mathrm{Ass}_{iso}(I) = \emptyset$. This decomposition is called* a pseudo-primary decomposition *in [26], where it is computed by separators from given $\mathrm{Ass}_{iso}(I)$. Meanwhile, we introduce another method to compute the minimal P-pseudo-primary components directly by using DIQ in Lemma 3.3.3. We note that the minimal P-pseudo-primary component is determined uniquely and has the P-isolated primary component of I as its component (see Lemma 1.2.3).*

Example 1.1.24. *For $I = \langle x^2(x+1), x(x+1)y\rangle = \langle x\rangle \cap \langle x+1\rangle \cap \langle x^2, y\rangle \subset \mathbb{Q}[x,y]$, $\langle x^2, xy\rangle$ is the minimal $\langle x\rangle$-pseudo-primary component of I and $\langle x+1\rangle$ is the minimal $\langle x+1\rangle$-pseudo-primary component of I.*

We may regard a P-pseudo-primary component as a "column localization" since it has different dimensional primary components in general. Conversely, we may consider a "row localization", that contains *equidimensional* primary components, that is, primary components with the same dimension. For a definition of the dimension of an ideal, see Definition 3.3.1 in [13].

Definition 1.1.25 ([10], Section 1)**.** *Let I be an ideal and $\mathcal{Q}$ a primary decomposition of I. We call* $\mathrm{hull}(I) = \bigcap_{Q \in \mathcal{Q}, \dim(Q) = \dim(I)} Q$ the equidimensional hull *of I. Since every primary component Q satisfying $\dim(Q) = \dim(I)$ is isolated, $\mathrm{hull}(I)$ is determined independently from the choice of primary decompositions.*

Example 1.1.26. *For $I = \langle x^4 - x^2, x^2y + xy\rangle = \langle x\rangle \cap \langle x+1\rangle \cap \langle x^2, y\rangle \cap \langle x-1, y\rangle \subset \mathbb{Q}[x,y]$, it follows that $\mathrm{hull}(I) = \langle x\rangle \cap \langle x+1\rangle$.*

Here, we define a *regular sequence* in I. Using a regular sequence in I, we can compute the "equidimensional hull" $\mathrm{hull}(I)$ of I (see Proposition 1.4.6). For computation of regular sequence, see Proposition 1.4.7.

Definition 1.1.27 (Regular sequence; [13], Definition 7.6.1)**.** *A sequence $a_1, \ldots, a_r \in K[X]$ is called a* regular sequence *if*

(1) a_i is not a zerodivisor for $K[X]/\langle a_1, \ldots, a_{i-1}\rangle$ for $i = 1, \ldots, r$,

(2) $\langle a_1, \ldots, a_r\rangle \neq K[X]$.

Example 1.1.28 ([13], Remark 7.6.2)**.** *A sequence $a_1 = x(y-1)$, $a_2 = y$, $a_3 = z(y-1)$ is a regular sequence in $K[x,y,z]$. On the other hand, a sequence a_1, a_3, a_2 is not regular.*

We define another *special localization* by *MIS*.

Definition 1.1.29 ([13], Definition 3.5.3)**.** *For a subset U of variables X and an ideal I, we call U a* maximal independent set (MIS) *of I if $K[U] \cap I = \{0\}$ and the cardinality of U is equal to the dimension of I.*

Remark 1.1.30. *For an MIS U of I, $IK[X]_{K[U]^\times}$ is a 0-dimensional ideal and $IK[X]_{K[U]^\times} \cap K[X]$ is the intersection of its primary components which have U as their MIS (see Proposition 1.4.9). Once we have a Gröbner basis of I, its MIS can be computed from one of $\langle \mathrm{lp}(G) \rangle$. For finding an MIS, see Exercise 3.52 in [13]. In particular, if I is a prime ideal, then it is easier to compute a MIS of I (see [5]).*

Example 1.1.31. *Let $I = \langle x^2, xy \rangle$. Then $U = \{y\}$ is an MIS of I and $I\mathbb{Q}[X]_{\mathbb{Q}[U]^\times} \cap \mathbb{Q}[X] = \langle x \rangle$.*

We define a special subset of $\mathrm{Ass}(I)$, which has a good relationship to *localization*. The localization with respect to an *isolated set* can be expressed as intersection of primary components whose prime divisors are in the isolated set. We note that $A(P)$, in Proposition 1.1.22, is an isolated set.

Definition 1.1.32 ([1], Chapter 4)**.** *Let I be an ideal. A subset $\mathcal{PP}$ of $\mathrm{Ass}(I)$ is said to be* isolated *if it satisfies the following condition: for a prime divisor $P' \in \mathrm{Ass}(I)$, if $P' \subset P$ for some $P \in \mathcal{PP}$, then $P' \in \mathcal{PP}$.*

1.2 Fundamental Lemmas

Here, we introduce fundamental lemmas for DIQ and our LPAs. The following lemma is an easy but fundamental criterion for primary component using localization.

Lemma 1.2.1 ([17], Lemma 4)**.** *Let I be an ideal and P its prime divisor. If S is a multiplicatively closed set with $P \cap S = \emptyset$ and Q is a P-primary ideal, then the following conditions are equivalent.*

(A) Q is a primary component of I.

(B) Q is a primary component of $IK[X]_S \cap K[X]$.

Proof. First, (A) implies (B) from Proposition 4.9 in [1]. For primary decompositions $\mathcal{Q}$ of I and $\mathcal{Q}'$ of $IK[X]_S \cap K[X]$ with $Q \in \mathcal{Q}'$, we obtain that $\{Q' \in \mathcal{Q} \mid Q' \cap S \neq \emptyset\} \cup \mathcal{Q}'$ is also a primary decomposition of I. Hence, (B) implies (A). □

In particular, one or more isolated primary components of I are isolated in $IK[X]_S \cap K[X]$ if the localization is not trivial.

Example 1.2.2. *For $I = \langle x^2, xy \rangle \subset K[X] = K[x, y]$, we obtain that $\langle x \rangle$ is the isolated primary component of both I and $IK[X]_{\langle x \rangle} \cap K[X] = \langle x \rangle$.*

The following lemma tells us a relationship between a localization and an isolated set (see Definition 1.1.32).

Lemma 1.2.3 ([1], Theorem 4.10)**.** *Let I be an ideal and $\mathcal{PP}$ an isolated set contained in $\mathrm{Ass}(I)$. For a multiplicatively closed set $S = K[X] \backslash \bigcup_{P \in \mathcal{PP}} P$ and a primary decomposition $\mathcal{Q}$ of I, $IK[X]_S \cap K[X] = \bigcap_{Q \in \mathcal{Q}, \sqrt{Q} \in \mathcal{PP}} Q$.*

Example 1.2.4. *For* $I = \langle x^2(x+1), x(x+1)y\rangle = \langle x\rangle \cap \langle x+1\rangle \cap \langle x^2, y\rangle \subset K[X] = K[x,y]$, $\mathcal{PP} = \{\langle x\rangle, \langle x, y\rangle\}$ *is an isolated subset of* $\mathrm{Ass}(I) = \{\langle x\rangle, \langle x+1\rangle, \langle x, y\rangle\}$. *Let* $S = K[X] \setminus \bigcup_{P\in\mathcal{PP}} P$. *Then,* $IK[X]_S \cap K[X] = \langle x^2, xy\rangle = \langle x\rangle \cap \langle x^2, y\rangle$.

The following lemma tells that primary ideals have a property similar to one of prime ideals.

Lemma 1.2.5 ([17], Lemma 16)**.** *Let* I *and* J *be ideals. Let* Q *be a primary ideal. If* $IJ \subset Q$ *and* $J \not\subset \sqrt{Q}$, *then* $I \subset Q$. *In particular, if* $I \cap J \subset Q$ *and* $J \not\subset \sqrt{Q}$, *then* $I \subset Q$.

Proof. Let $f \in I$ and $g \in J \setminus \sqrt{Q}$. Since Q is $\sqrt{Q}$-primary, $fg \in IJ \subset Q$ implies $f \in Q$. □

Example 1.2.6. *Let* $I = \langle x\rangle$, $J = \langle x+1\rangle$ *and* $Q = \langle x, y^2\rangle$. *Then,* $I \cap J \subset \langle x(x+1)\rangle \subset \langle x, y^2\rangle = Q$ *and* $J = \langle x+1\rangle \not\subset \sqrt{Q} = \langle x, y\rangle$. *Thus,* $I = \langle x\rangle \subset Q = \langle x, y^2\rangle$.

Next, we remark the "splitting tool", one of the most important tool for primary decomposition.

Lemma 1.2.7 ([28], Proposition 3.53)**.** *Let* I *and* J *be ideals. Then, for a sufficiently large integer* m,

$$I = (I : J^\infty) \cap (I + J^m).$$

where $J^m = \langle f_1 \cdots f_m \mid f_1, \ldots, f_m \in J\rangle$ *(if* J *is generated by* F, *then* $J^m = \langle f_1 \cdots f_m \mid f_1, \ldots, f_m \in F\rangle$*).*

Example 1.2.8. *For* $I = \langle x^2, xy\rangle = \langle x\rangle \cap \langle x^2, y\rangle$ *and* $J = \langle x, y\rangle$, *it follows that* $J^2 = \langle x^2, xy, y^2\rangle$ *and*

$$I = (I : J^\infty) \cap (I + J^2) = \langle x\rangle \cap \langle x^2, xy, y^2\rangle.$$

Also, we recall the famous *Prime Avoidance Lemma*.

Lemma 1.2.9 ([1], Proposition 1.11)**.** (i) *Let* $P_1, \ldots, P_m$ *be prime ideals and let* I *be an ideal contained in* $\bigcup_{i=1}^m P_i$. *Then,* $I \subset P_i$ *for some* i.
(ii) *Let* $I_1, \ldots, I_m$ *be ideals and let* P *be a prime ideal containing* $\bigcap_{i=1}^m I_i$. *Then* $P \supset I_i$ *for some* i. *If* $P = \bigcap_{i=1}^m I_i$, *then* $P = I_i$ *for some* i.

Finally, we introduce fundamental properties of *ideal quotient*. The first two statements in Lemma 1.2.10 can be seen in several papers and books ([1], Lemma 4.4. [13], Lemma 4.1.3. [28], the remark before Proposition 3.56).

Lemma 1.2.10 ([17], Lemma 19)**.** *Let* I *and* J *be ideals,* Q *a primary ideal and* $\mathcal{Q}$ *a primary decomposition of* I. *Then,*

$$(Q : J) = \begin{cases} Q & (J \not\subset \sqrt{Q}), \\ K[X] & (J \subset Q), \\ \sqrt{Q}\text{-primary ideal properly containing } Q & (J \not\subset Q, J \subset \sqrt{Q}), \end{cases} \tag{1.1}$$

$$(Q : J^\infty) = \begin{cases} Q & (J \not\subset \sqrt{Q}), \\ K[X] & (J \subset \sqrt{Q}), \end{cases} \tag{1.2}$$

$$(I : J) = \bigcap_{Q\in\mathcal{Q}, J\not\subset\sqrt{Q}} Q \cap \bigcap_{Q\in\mathcal{Q}, J\not\subset Q, J\subset\sqrt{Q}} (Q : J), \tag{1.3}$$

$$(I : J^\infty) = (I : \sqrt{J}^\infty) = \bigcap_{Q\in\mathcal{Q}, J\not\subset\sqrt{Q}} Q. \tag{1.4}$$

Proof. We omit proofs of (1.1) and (1.2). First, we prove (1.3). From $I = \bigcap_{Q\in\mathcal{Q}} Q$ and (1.1), we obtain that

$$\begin{aligned}(I : J) &= (\bigcap_{Q\in\mathcal{Q}} Q : J) = \bigcap_{Q\in\mathcal{Q}} (Q : J)\\ &= \bigcap_{Q\in\mathcal{Q},J\not\subset\sqrt{Q}} (Q : J) \cap \bigcap_{Q\in\mathcal{Q},J\not\subset Q,J\subset\sqrt{Q}} (Q : J) \cap \bigcap_{Q\in\mathcal{Q},J\subset Q} (Q : J)\\ &= \bigcap_{Q\in\mathcal{Q},J\not\subset\sqrt{Q}} Q \cap \bigcap_{Q\in\mathcal{Q},J\not\subset Q,J\subset\sqrt{Q}} (Q : J) \cap K[X]\\ &= \bigcap_{Q\in\mathcal{Q},J\not\subset\sqrt{Q}} Q \cap \bigcap_{Q\in\mathcal{Q},J\not\subset Q,J\subset\sqrt{Q}} (Q : J).\end{aligned}$$

Second, we show (1.4). From $I = \bigcap_{Q\in\mathcal{Q}} Q$ and (1.2), we obtain that

$$\begin{aligned}(I : J^\infty) &= \bigcap_{Q\in\mathcal{Q},J\not\subset\sqrt{Q}} (Q : J^\infty) \cap \bigcap_{Q\in\mathcal{Q},J\subset\sqrt{Q}} (Q : J^\infty)\\ &= \bigcap_{Q\in\mathcal{Q},J\not\subset\sqrt{Q}} Q \cap K[X] = \bigcap_{Q\in\mathcal{Q},J\not\subset\sqrt{Q}} Q.\end{aligned}$$

Since $J \subset \sqrt{Q}$ is equivalent to $\sqrt{J} \subset \sqrt{Q}$, we obtain that $(I : J^\infty) = (I : \sqrt{J}^\infty)$. □

1.3 Additional Definitions and Lemmas

Next, we introduce the notion of hull-primary ideal, which is an extension of the definition of pseudo-primary ideal. We use hull-primary ideal in Section 4.2.1 to devise practical techniques for LPAs.

Definition 1.3.1 ([17], Definition 13)**.** *Let I be an ideal. We say that I is* hull-primary *if* $\mathrm{hull}(I)$ *is a primary ideal. For a prime ideal P, we say that a hull-primary ideal I is P-*hull-primary *if* $P = \mathrm{hull}(\sqrt{I})$.

Example 1.3.2. *Let $I = \langle x^3 - x^2y, x^2y^2 + x^2y\rangle = \langle x^2\rangle \cap \langle x^3, y\rangle \cap \langle x+1, y+1\rangle \subset \mathbb{Q}[x, y]$. Since $\mathrm{hull}(I) = \langle x^2\rangle$ is $\langle x\rangle$-primary, I is $\langle x\rangle$-hull primary.*

As a pseudo-primary ideal has the unique isolated component, we remark following.

Remark 1.3.3. *Every pseudo-primary ideal is hull-primary.*

Example 1.3.4. *$I = \langle x^2, xy\rangle = \langle x\rangle \cap \langle x^2, y\rangle$ is $\langle x\rangle$-pseudo-primary and thus $\langle x\rangle$-hull-primary.*

Using the following lemma and a variant of DIQ, we can compute the isolated P-primary component of I in Chapter 4.

Lemma 1.3.5 ([17], Lemma 15)**.** *Let P be an isolated prime divisor of I and $\overline{Q}_P$ the minimal P-pseudo-primary component of I. Then, $\overline{Q}_P$ is P-hull-primary and $\mathrm{hull}(\overline{Q}_P)$ is the isolated P-primary component of I.*

Proof. By Remarks 1.1.23 and 1.3.3, it follows that $\overline{Q}_P$ is P-hull-primary and $\mathrm{hull}(\overline{Q}_P)$ is the isolated P-primary component. By the definition of $\overline{Q}_P$ and Lemma 1.2.1, we obtain that $\mathrm{hull}(\overline{Q}_P)$ is the isolated P-primary component of I. □

Example 1.3.6. *Let $I = \langle x^2, xy^2 + xy\rangle = \langle x\rangle \cap \langle x^2, y\rangle \cap \langle x^2, y+1\rangle \subset \mathbb{Q}[x,y]$. For $P = \langle x\rangle$, $\overline{Q}_P = \langle x\rangle \cap \langle x^2, y\rangle$ is the minimal P-pseudo primary component of I and $\mathrm{hull}(\overline{Q}_P) = \langle x\rangle$ is the P-isolated primary component of I.*

The following lemma tells us when primary component intersects a multiplicatively closed set. It is used to prove Lemma 3.1.3, a criterion for localization.

Lemma 1.3.7 ([17], Lemma 7)**.** *Let $\mathcal{Q}$ be a primary decomposition of I and $Q \in \mathcal{Q}$. For a multiplicatively closed set S, the following conditions are equivalent.*
(A) $IK[X]_S \cap K[X] \subset IK[X]_{\sqrt{Q}} \cap K[X]$.
(B) $Q \cap S = \emptyset$.

Proof. Show that (A) implies (B). As $IK[X]_{\sqrt{Q}} \cap K[X] \subset Q$, $IK[X]_S \cap K[X] = \bigcap_{Q' \in \mathcal{Q}, Q' \cap S = \emptyset} Q' \subset Q$. Since $\mathcal{Q}$ is irredundant, $IK[X]_S \cap K[X]$ has $\sqrt{Q}$-primary component. Thus, $Q \cap S = \emptyset$. Now, we show that (B) implies (A). Then, $\sqrt{Q} \cap S = \emptyset$ and $Q' \cap S = \emptyset$ for any $Q' \in \mathcal{Q}$ s.t. $Q' \subset \sqrt{Q}$. Thus, $IK[X]_{\sqrt{Q}} \cap K[X] = \bigcap_{Q' \subset \sqrt{Q}} Q'$ implies $IK[X]_S \cap K[X] \subset IK[X]_{\sqrt{Q}} \cap K[X]$. □

Example 1.3.8. *For $I = \langle x^3 + x^2, x^2y + xy\rangle = \langle x\rangle \cap \langle x+1\rangle \cap \langle x^2, y\rangle \subset \mathbb{Q}[X] = \mathbb{Q}[x,y]$, let $S = \mathbb{Q}[X] \setminus \langle x, y\rangle$. Then, $I\mathbb{Q}[X]_S \cap \mathbb{Q}[X] = \langle x\rangle \cap \langle x^2, y\rangle \subset I\mathbb{Q}[X]_{\sqrt{\langle x\rangle}} \cap \mathbb{Q}[X] = \langle x\rangle$ and $\langle x\rangle \cap S = \emptyset$. On the other hand, $I\mathbb{Q}[X]_S \cap \mathbb{Q}[X] = \langle x\rangle \cap \langle x^2, y\rangle \not\subset I\mathbb{Q}[X]_{\sqrt{\langle x+1\rangle}} \cap \mathbb{Q}[X] = \langle x+1\rangle$ and $\langle x+1\rangle \cap S \neq \emptyset$.*

Hull-primary ideals have a similar property to one of primary ideals as follows.

Lemma 1.3.9 ([17], Lemma 17)**.** *Let I be a P-hull-primary and Q a P-primary ideal. If $I \subset Q$, then $\mathrm{hull}(I) \subset Q$.*

Proof. If $I = \mathrm{hull}(I)$, then $\mathrm{hull}(I) = I \subset Q$. Thus, we assume $I \neq \mathrm{hull}(I)$. Let $\mathcal{Q}$ be a primary decomposition of I and $J = \bigcap_{Q' \in \mathcal{Q}, Q' \neq \mathrm{hull}(I)} Q'$. Then $I = \mathrm{hull}(I) \cap J \subset Q$ and $J \not\subset P$. Since Q is P-primary, we obtain that $\mathrm{hull}(I) \subset Q$ by Lemma 1.2.5. □

Example 1.3.10. *Let $I = \langle x^3 - x^2y, x^2y^2 + x^2y\rangle = \langle x^2\rangle \cap \langle x^3, y\rangle \cap \langle x+1, y+1\rangle$ and $Q = \langle x\rangle$. Then, $I \subset Q$ and $\mathrm{hull}(Q) = \langle x^2\rangle \subset Q$.*

1.4 Computations of Basic Ideal Operations

In the rest of this section, we see some computations of basic ideal operations such as intersection of ideal, ideal quotient, saturation, radical of ideal and primary decomposition.

Proposition 1.4.1 ([13], Lemma 1.8.10)**.** *For ideals $I = \langle f_1, \ldots, f_r\rangle$, $J = \langle g_1, \ldots, g_s\rangle$ and a new variable t,*

$$I \cap J = (\langle t\rangle I + \langle 1-t\rangle J) \cap K[X]$$

where $\langle t\rangle I + \langle 1-t\rangle J$ is the ideal generated by $\{tf_1, \ldots, tf_r, (1-t)g_1, \ldots, (1-t)g_s\}$ in $K[X,t]$. For a Gröbner basis G of $\langle t\rangle I + \langle 1-t\rangle J$ with respect to a (block) monomial ordering with $\{t\} \succ\succ X$, $G \cap K[X]$ is a Gröbner basis of $I \cap J$. Thus, the intersection of ideals is computable.

Next, ideal quotient can be computed by the following ways.

Proposition 1.4.2 ([13], Lemma 1.8.12 (Solution 1)). *For an ideal I and a polynomial f,*

$$(I : \langle f \rangle) = (I \cap \langle f \rangle) \cdot f^{-1} = \{gf^{-1} \mid g \in I \cap \langle f \rangle\}.$$

Then, $(I : \langle f \rangle)$ can be computed by Gröbner bases computations. Moreover, for an ideal $J = \langle f_1, \ldots, f_r \rangle$

$$(I : J) = \bigcap_{i=1}^{r} (I : \langle f_i \rangle)$$

and thus the ideal quotient of ideals is computable.

We can obtain a generating set of the ideal quotient in another manner as follows.

Proposition 1.4.3 ([28], Proposition 2.10). *For ideals I and $J = \langle f_1, \ldots, f_r \rangle$, a new variable t and $f = f_1 + f_2 t + \cdots + f_r t^{r-1}$,*

$$(I : J) = (IK[X, t] : \langle f \rangle) \cap K[X].$$

By using ideal quotient, we obtain a generating set of saturation as the following proposition.

Remark 1.4.4. *Let I and J be ideals. Then, by the Noetherian property of $K[X]$, for a sufficiently large integer m,*

$$(I : J^{\infty}) = (I : J^m) = (I : J^{m+1}) = \cdots .$$

Thus, the saturation is computable.

We can also compute *saturation* in the following manner.

Proposition 1.4.5 ([28], Proposition 2.12). *For ideals I and $J = \langle f_1, \ldots, f_r \rangle$, a new variable t and $f = f_1 + f_2 t + \cdots + f_r t^{r-1}$,*

$$(I : J^{\infty}) = ((I + \langle t - f \rangle) : \langle t \rangle^{\infty}) \cap K[X].$$

For a given I, $\mathrm{hull}(I)$ can be computed in several manners. For instance, it can be computed by Ext functors $\mathrm{Ext}_{K[X]}(K[X]/I, K[X])$ (see [10]), or a *regular sequence* (see Definition 1.1.27) contained in I (see [28]) as follows. In general, the computation of Ext functors tends to be time-consuming, compared with ideal computations. Thus, in this thesis, we use a regular sequence or an MIS to compute equidimensional hull.

Proposition 1.4.6 ([28], Proposition 3.41). *Let I be an ideal in $K[x_1, \ldots, x_n]$ and $u \subset I$ a regular sequence of length c, where c is the codimension of I i.e. $c = n - \dim(I)$. Then* $\mathrm{hull}(I) = (\langle u \rangle : (\langle u \rangle : I))$.

For a computation of a regular sequence in I, we can use the following criterion. For a modified computation of a regular sequence in a pseudo-primary ideal, see Lemma 4.2.5.

Lemma 1.4.7 ([28], Proposition 2.9). *Let I be an ideal. For $f \in K[X]$, f is not a zero-divisor for $K[X]/I$ if and only if $(I : \langle f \rangle) = I$. Consequently, $a_1, \ldots, a_r$ is a regular sequence in $K[X]$ if and only if*

(1) $(\langle a_1, \ldots, a_{i-1} \rangle : \langle a_i \rangle) = \langle a_1, \ldots, a_{i-1} \rangle$ *for each i,*

(2) $\langle a_1, \ldots, a_r \rangle \neq K[X]$.

If I is 0-dimensional and K is a perfect field, then we can compute the radical of I by the following.

Proposition 1.4.8 ([28], Theorem 4.16)**.** *Let I be a 0-dimensional ideal in $K[X]$, where K is a perfect field. There is a univariate polynomial $f_i(x_i)$ such that $I \cap K[x_i] = \langle f_i \rangle$ for $i = 1, \ldots, n$ and let g_i be the squarefree part of f_i i.e. $g_i = h_{i1} \cdots h_{ir_i}$ where $f_i = h_{i1}^{e_1} \cdots h_{ir_i}^{e_{r_i}}$ is an irreducible factorization of f_i over K. Then*

$$\sqrt{I} = I + \langle g_1, \ldots, g_n \rangle.$$

Since each f_i can be computed from the reduced Gröbner basis of I, the radical is computable.

In case that I is not 0-dimensional, we may reduce it to 0-dimensional case by localization using MIS. If the characteristic of K is positive, then we can use the *preimage* of Frobenius map.

Proposition 1.4.9 ([13], Proposition 4.3.1)**.** *Let I be an ideal and $U \subset X$ an MIS of I. Then,*

(1) *$IK(U)[X \setminus U]$ is a 0-dimensional ideal of $K(U)[X \setminus U]$.*

(2) *For a Gröbner basis $G = \{f_1, \ldots, f_s\}$ of $IK(U)[X \setminus U]$ with $G \subset I$ and $h = \mathrm{lcm}(\mathrm{lc}(f_1), \ldots, \mathrm{lc}(f_s)) \in K(U)$,*

$$IK(U)[X \setminus U] \cap K[X] = (I : \langle h \rangle^{\infty}).$$

(3) *If $\mathcal{Q}'$ is a primary decomposition of $IK(U)[X \setminus U]$, then $\{Q' \cap K[X] \mid Q' \in \mathcal{Q}'\}$ is a primary decomposition of $IK(U)[X \setminus U] \cap K[X]$.*

If a given ideal is 0-dimensional, we can compute its primary decomposition from the factorization of a polynomial in I. For a definition of *general position*, see Definition 4.2.1 in [13].

Proposition 1.4.10 ([13], Proposition 4.2.3)**.** *Let I be a 0-dimensional ideal in $\mathbb{Q}[X]$. Then, for $f \in I \cap K[x_n]$ and an irreducible factorization $f = f_1^{e_1} \cdots f_s^{e_s}$,*

$$I = (I + \langle f_1^{e_1} \rangle) \cap (I + \langle f_2^{e_2} \rangle) \cap \cdots \cap (I + \langle f_s^{e_s} \rangle).$$

If I is in general position with respect to the lexicographic ordering with $x_1 \succ \cdots \succ x_n$, it gives a primary decomposition.

Finally, we recall some algorithms of primary decomposition. First, we provide the sketch of a generalized version of Gianni-Trager-Zacharias algorithm ([5, 12, 13]) as follows.

Generalized version of Gianni-Trager-Zacharias algorithm (GTZ)

Input: F: a generating set of an ideal I in $\mathbb{Q}[X]$
Output: $\mathcal{Q}$: a primary decomposition of I

$\mathcal{Q} \leftarrow \{\}$
Find an MIS U of I
Compute $h \in K[X]$ and a positive integer m s.t. $IK(U)[X \setminus U] \cap K[X] = (I : \langle h \rangle^{\infty}) = (I : \langle h^m \rangle)$
Compute a general primary decomposition $\mathcal{Q}'$ of $IK(U)[X \setminus U]$ as a 0-dimensional ideal by Proposition 1.4.9 and Proposition 1.4.10
$\mathcal{Q}'_c \leftarrow \{Q \cap K[X] \mid Q \in \mathcal{Q}'\}$
$\mathcal{Q} \leftarrow \mathcal{Q} \cup \mathcal{Q}'_c$
IF $(I : h^{\infty}) \not\subset I + \langle h^m \rangle$ THEN
$\mathcal{Q} \leftarrow \mathcal{Q} \cup \mathrm{GTZ}(I + \langle h^m \rangle)$
Delete unnecessary components in $\mathcal{Q}$
RETURN $\mathcal{Q}$

Second, we introduce Shimoyama-Yokoyama algorithm [26], which uses the prime decomposition of the radical of the ideal.

Shimoyama-Yokoyama algorithm (SY)

Input: F: a generating set of an ideal I in $\mathbb{Q}[X]$
Output: $\mathcal{Q}$: a primary decomposition of I

$\mathcal{Q} \leftarrow \{\}$
Compute the prime decomposition $\mathcal{PP}$ of $\sqrt{I}$ by some efficient methods
Compute a pseudo-primary decomposition $I = \overline{Q}_1 \cap \cdots \cap \overline{Q}_r \cap I'$ from $\mathcal{PP}$
Compute the isolated primary component Q_i of $\overline{Q}_i$ and $\mathcal{Q} \leftarrow \mathcal{Q} \cup \{Q_i\}$
IF $\overline{Q}_1 \cap \cdots \cap \overline{Q}_r \not\subset I'$ THEN
$\mathcal{Q} \leftarrow \mathcal{Q} \cup SY(I')$
Delete unnecessary components in $\mathcal{Q}$
RETURN $\mathcal{Q}$

Remark 1.4.11. *Effective localization was first introduced in [26]. As mentioned in Remark 1.1.23, it uses* separators *to compute a pseudo-primary decomposition. Effective localization can compute necessary primary components for the localization of I by some prime ideal. Also, we can avoid generating unnecessary primary ideals by Kawazoe-Noro Algorithm [19].*

Remark 1.4.12. *If an ideal is zero-dimensional, we can apply so-called FGLM-algorithm as an efficient algorithm (see [11]). In case that the coefficient field has a valuation (e.g. the p-adic field), we can define* tropical Gröbner basis *(see [16]).*

Chapter 2

Double Ideal Quotient

In this chapter, we introduce notions and properties of DIQ and its variants. DIQ has already appeared in [28] to check associated primes or compute equidimensional hulls (see Proposition 1.4.6). In Chapter 3, we investigate DIQ and its variants more deeply and provide new criteria for prime divisors and primary components by using DIQ and its variants.

2.1 Fundamental Properties of Double Ideal Quotient

Double Ideal Quotient (DIQ) is an ideal of shape $(I : (I : J))$ where I and J are ideals. For an ideal I and its primary decomposition $\mathcal{Q}$, we divide $\mathcal{Q}$ into three parts:

$$\begin{aligned}
\mathcal{Q}_1(J) &= \{Q \in \mathcal{Q} \mid J \not\subset \sqrt{Q}\},\\
\mathcal{Q}_2(J) &= \{Q \in \mathcal{Q} \mid J \subset Q\},\\
\mathcal{Q}_3(J) &= \{Q \in \mathcal{Q} \mid J \not\subset Q, J \subset \sqrt{Q}\}.
\end{aligned}$$

Example 2.1.1. *Let $I = \langle x^3y, x^2y^2\rangle = \langle x^2\rangle \cap \langle x^3, y^2\rangle \cap \langle y\rangle$, $J = \langle x^2\rangle$ and $\mathcal{Q} = \{\langle x^2\rangle, \langle x^3, y^2\rangle, \langle y\rangle\}$ a primary decomposition of I. It follows that $\mathcal{Q}_1(J) = \{\langle y\rangle\}$, $\mathcal{Q}_2(J) = \{\langle x^2\rangle\}$, and $\mathcal{Q}_3(J) = \{\langle x^3, y^2\rangle\}$.*

Then, our DIQ is expressed precisely by components of them. The following proposition can be proved directly from Lemma 1.2.10.

Proposition 2.1.2 ([17], Proposition 20)**.** *Let I and J be ideals. Then,*

$$\begin{aligned}
(I : (I : J)) &= \bigcap_{Q\in\mathcal{Q}_2(J)} \left(Q : \Big(\bigcap_{Q'\in\mathcal{Q}_1(J)} Q' \cap \bigcap_{Q'\in\mathcal{Q}_3(J)} (Q' : J)\Big)\right) \qquad (2.1)\\
&\quad \cap \bigcap_{Q\in\mathcal{Q}_3(J)} \left(Q : \Big(\bigcap_{Q'\in\mathcal{Q}_1(J)} Q' \cap \bigcap_{Q'\in\mathcal{Q}_3(J)} (Q' : J)\Big)\right),\\
\sqrt{(I : (I : J))} &= \bigcap_{P\in\mathrm{Ass}(I), J\subset P} P. \qquad (2.2)
\end{aligned}$$

Proof. First, we show (2.1). We divide I into three parts:

$$I = \bigcap_{Q\in\mathcal{Q}_1(J)} Q \cap \bigcap_{Q\in\mathcal{Q}_2(J)} Q \cap \bigcap_{Q\in\mathcal{Q}_3(J)} Q.$$

Then,

$$\begin{aligned}(I:(I:J)) &= \left([\bigcap_{Q\in\mathcal{Q}_1(J)} Q \cap \bigcap_{Q\in\mathcal{Q}_2(J)} Q \cap \bigcap_{Q\in\mathcal{Q}_3(J)} Q] : (I:J)\right) \\ &= (\bigcap_{Q\in\mathcal{Q}_1(J)} Q:(I:J)) \cap (\bigcap_{Q\in\mathcal{Q}_2(J)} Q:(I:J)) \cap (\bigcap_{Q\in\mathcal{Q}_3(J)} Q:(I:J)).\end{aligned}$$

Since

$$(I:J) = \bigcap_{Q'\in\mathcal{Q}_1(J)} Q' \cap \bigcap_{Q'\in\mathcal{Q}_3(J)} (Q':J),$$

we obtain that

- $$\begin{aligned}(\bigcap_{Q\in\mathcal{Q}_1(J)} Q:(I:J)) &= (\bigcap_{Q\in\mathcal{Q}_1(J)} Q:(\bigcap_{Q'\in\mathcal{Q}_1(J)} Q' \cap \bigcap_{Q'\in\mathcal{Q}_3(J)} (Q':J))) \\ &= K[X]\end{aligned}$$

- $$\begin{aligned}(\bigcap_{Q\in\mathcal{Q}_2(J)} Q:(I:J)) &= (\bigcap_{Q\in\mathcal{Q}_2(J)} Q:(\bigcap_{Q'\in\mathcal{Q}_1(J)} Q' \cap \bigcap_{Q'\in\mathcal{Q}_3(J)} (Q':J))) \\ &= \bigcap_{Q\in\mathcal{Q}_2(J)} (Q:(\bigcap_{Q'\in\mathcal{Q}_1(J)} Q' \cap \bigcap_{Q'\in\mathcal{Q}_3(J)} (Q':J)))\end{aligned}$$

- $$\begin{aligned}(\bigcap_{Q\in\mathcal{Q}_3(J)} Q:(I:J)) &= (\bigcap_{Q\in\mathcal{Q}_3(J)} Q:(\bigcap_{Q'\in\mathcal{Q}_1(J)} Q' \cap \bigcap_{Q'\in\mathcal{Q}_3(J)} (Q':J))) \\ &= \bigcap_{Q\in\mathcal{Q}_3(J)} (Q:(\bigcap_{Q'\in\mathcal{Q}_1(J)} Q' \cap \bigcap_{Q'\in\mathcal{Q}_3(J)} (Q':J))).\end{aligned}$$

The second property (2.2) can be proved directly from the property (2.1) and the irredundance of the primary decomposition $\mathcal{Q}$. □

This proposition can be used to prove the following known criterion for prime divisors. We note that $P \supset (I:(I:P))$ is equivalent to $P = (I:(I:P))$ (see Remark 5.1.1).

Corollary 2.1.3 ([28], Corollary 3.4)**.** *Let I be an ideal and P a prime ideal. Then, P belongs to* $\mathrm{Ass}(I)$ *if and only if $P \supset (I:(I:P))$.*

Proof. We note $P \supset (I:(I:P))$ if and only if $P \supset \sqrt{(I:(I:P))}$. By Proposition 2.1.2, $\sqrt{(I:(I:P))} = \bigcap_{P'\in\mathrm{Ass}(I), P\subset P'} P'$. If $P \in \mathrm{Ass}(I)$, then $\sqrt{(I:(I:P))} = \bigcap_{P'\in\mathrm{Ass}(I), P\subset P'} P' \subset P$. On the other hand, if $P \supset \sqrt{(I:(I:P))}$, then there is $P' \in \mathrm{Ass}(I)$ s.t. $P' \subset P$ and $P' \supset P$ by the Prime Avoidance Lemma (see Lemma 1.2.9). Thus $P = P' \in \mathrm{Ass}(I)$. □

Example 2.1.4. *Let $I = \langle x^2, xy\rangle = \langle x\rangle \cap \langle x^2, y\rangle$ in $\mathbb{Q}[x,y]$. Then, $P = \langle x\rangle$ is a prime divisor of I and $(I:(I:P)) = (I:\langle x,y\rangle) = \langle x\rangle \subset P$.*

2.2 Variants of Double Ideal Quotient

Replacing *ideal quotient* with *saturation* in DIQ, we have the following variants.

Definition 2.2.1 (Variants of DIQ; [18], Definition 22)**.** *We call* $(I : (I : J)^\infty)$ the first saturated quotient*,* $(I : (I : J^\infty)^\infty)$ the second saturated quotient*, and* $(I : (I : J^\infty))$ the third saturated quotient *respectively.*

In the following proposition, we can see that variants of DIQ have useful information about localization.

Proposition 2.2.2 ([17], Proposition 22)**.** *Let* $\mathcal{Q}$ *be a primary decomposition of* I*. Then,*

$$(I : (I : J)^\infty) = \bigcap_{Q \in \mathcal{Q}, J \subset IK[X]_{\sqrt{Q}} \cap K[X]} Q, \tag{2.3}$$

$$(I : (I : J^\infty)^\infty) = \bigcap_{Q \in \mathcal{Q}, J \subset \sqrt{IK[X]_{\sqrt{Q}} \cap K[X]}} Q, \tag{2.4}$$

$$(I : (I : J^\infty)) = \bigcap_{Q \in \mathcal{Q}_2(J)} (Q : \bigcap_{Q' \in \mathcal{Q}_1(J)} Q') \cap \bigcap_{Q \in \mathcal{Q}_3(J)} (Q : \bigcap_{Q' \in \mathcal{Q}_1(J)} Q'). \tag{2.5}$$

Proof. Here, we give an outline of the proof. The formula (2.3) can be proved by combining the equation

$$(I : (I : J)^\infty) = (I : \sqrt{(I : J)}^\infty) = \bigcap_{Q \in \mathcal{Q}, \bigcap_{Q' \in \mathcal{Q}_1(J)} \sqrt{Q'} \cap \bigcap_{Q' \in \mathcal{Q}_3(J)} \sqrt{Q'} \not\subset \sqrt{Q}} Q$$

by Lemma 1.2.10 and the following equivalence

(1-a) $J \subset IK[X]_{\sqrt{Q}} \cap K[X]$.

(1-b) $\bigcap_{Q' \in \mathcal{Q}_1(J)} \sqrt{Q'} \cap \bigcap_{Q' \in \mathcal{Q}_3(J)} \sqrt{Q'} \not\subset \sqrt{Q}$.

for each $Q \in \mathcal{Q}$. The second formula (2.4) can be proved by combining the equation $(I : (I : J^\infty)^\infty) = (I : (I : J^m)^\infty) = \bigcap_{Q \in \mathcal{Q}, J^m \subset IK[X]_{\sqrt{Q}} \cap K[X]} Q$ for a sufficiently large integer m from the first formula (2.3), and the following equivalence

(2-a) $J^m \subset IK[X]_{\sqrt{Q}} \cap K[X]$ for a sufficiently large integer m.

(2-b) $J \subset \sqrt{IK[X]_{\sqrt{Q}} \cap K[X]}$.

for each $Q \in \mathcal{Q}$. The third formula (2.5) can be proved directly from Lemma 1.2.10.

Now, we explain some details. We show that (1-a) implies (1-b). If

$$\bigcap_{Q' \in \mathcal{Q}_1(J)} \sqrt{Q'} \cap \bigcap_{Q' \in \mathcal{Q}_3(J)} \sqrt{Q'} \subset \sqrt{Q},$$

then by Lemma 1.2.9, $\sqrt{Q'} \subset \sqrt{Q}$ for some $Q' \in \mathcal{Q}_1(J) \cup \mathcal{Q}_3(J)$. Since $Q' \subset \sqrt{Q'} \subset \sqrt{Q}$, we obtain that $IK[X]_{\sqrt{Q}} \cap K[X] = \bigcap_{Q'' \in \mathcal{Q}, Q'' \subset \sqrt{Q}} Q'' \subset Q'$. However, since $Q' \in \mathcal{Q}_1(J) \cup \mathcal{Q}_3(J)$, we obtain that $J \not\subset Q'$ and this contradicts $J \subset IK[X]_{\sqrt{Q}} \cap K[X] \subset Q'$.

Show that (1-b) implies (1-a). Let $Q' \in \mathcal{Q}$ contained $\sqrt{Q}$. Since $\bigcap_{Q'' \in \mathcal{Q}_1(J)} \sqrt{Q''} \cap \bigcap_{Q'' \in \mathcal{Q}_3(J)} \sqrt{Q''} \not\subset \sqrt{Q}$, we obtain that $Q' \notin \mathcal{Q}_1(J) \cup \mathcal{Q}_3(J)$ and $Q' \in \mathcal{Q}_2(J)$. Hence, $J \subset Q'$ and $J \subset \bigcap_{Q' \subset \sqrt{Q}} Q' = IK[X]_{\sqrt{Q}} \cap K[X]$.

Trivially, (2-a) implies (2-b) since $J \subset \sqrt{J^m} \subset \sqrt{IK[X]_{\sqrt{Q}} \cap K[X]}$. Show that (2-b) implies (2-a). For $Q \in \mathcal{Q}_2(J) \cup \mathcal{Q}_3(J)$, let $m_Q = \min\{m \mid J^m \subset Q\}$ and $m = \max\{m_Q \mid Q \in \mathcal{Q}_2(J) \cup \mathcal{Q}_3(J)\}$. Then, $(I : J^\infty) = (I : J^m)$. Since $IK[X]_{\sqrt{Q}} \cap K[X] = \bigcap_{Q' \in \mathcal{Q}, Q' \subset \sqrt{Q}} Q'$, we obtain that $Q' \in \mathcal{Q}_2(J) \cup \mathcal{Q}_3(J)$ for any $Q' \in \mathcal{Q}$ contained in $\sqrt{Q}$. Thus, we obtain that $J^m \subset IK[X]_{\sqrt{Q}} \cap K[X]$.

Finally, we show (2.5). Since $(I : J^\infty) = \bigcap_{Q' \in \mathcal{Q}_1(J)} Q'$ (see Lemma 1.2.10 (1.4)), we obtain that

$$\begin{aligned}(I : (I : J^\infty)) &= (I : \bigcap_{Q' \in \mathcal{Q}_1(J)} Q') \\ &= (\bigcap_{Q \in \mathcal{Q}_1(J)} Q \cap \bigcap_{Q \in \mathcal{Q}_2(J)} Q \cap \bigcap_{Q \in \mathcal{Q}_3(J)} Q : \bigcap_{Q' \in \mathcal{Q}_1(J)} Q') \\ &= \bigcap_{Q \in \mathcal{Q}_2(J)} (Q : \bigcap_{Q' \in \mathcal{Q}_1(J)} Q') \cap \bigcap_{Q \in \mathcal{Q}_3(J)} (Q : \bigcap_{Q' \in \mathcal{Q}_1(J)} Q').\end{aligned}$$

□

Example 2.2.3. *For* $I = \langle x^2y^3z, x^2y^2z^2, x^4z, x^3z^2\rangle = \langle x^2\rangle \cap \langle x^3, y^2\rangle \cap \langle x^4, y^3, z^2\rangle \cap \langle z\rangle$ *in* $K[x, y, z]$ *and* $J = \langle x^2\rangle$*, we have* $(I : J) = \langle x, y^2\rangle \cap \langle x^2, y^3, z^2\rangle \cap \langle z\rangle$ *and* $(I : J^\infty) = \langle z\rangle$*. Then*

$$\begin{aligned}(I : (I : J)^\infty) &= \bigcap_{Q \in \mathcal{Q}, J \subset IK[X]_{\sqrt{Q}} \cap K[X]} Q = \langle x^2\rangle, \\ (I : (I : J^\infty)^\infty) &= \bigcap_{Q \in \mathcal{Q}, J \subset \sqrt{IK[X]_{\sqrt{Q}} \cap K[X]}} Q = \langle x^2\rangle \cap \langle x^3, y^2\rangle, \\ (I : (I : J^\infty)) &= \bigcap_{Q \in \mathcal{Q}_2(J)} (Q : \bigcap_{Q' \in \mathcal{Q}_1(J)} Q') \cap \bigcap_{Q \in \mathcal{Q}_3(J)} (Q : \bigcap_{Q' \in \mathcal{Q}_1(J)} Q') = \langle x^2\rangle \cap \langle x^3, y^2\rangle \cap \langle x^4, y^3, z\rangle.\end{aligned}$$

Here, the first and second saturated quotients are intersections of primary components of I*, on the other hand, the third saturated quotient has a primary component which cannot be one of* I*.*

Using the first saturated quotient, we devise criteria for primary components in Chapter 3. The second saturated quotient can be used to an isolated prime divisors check and generate an isolated primary component in Chapter 4. The third saturated quotient gives another prime divisor criterion (Criterion 5 in Chapter 3) by the following proposition.

Proposition 2.2.4 ([17], Proposition 23)**.** *Let* I *and* J *be ideals. Then*

$$\sqrt{(I : (I : J^\infty))} = \bigcap_{P \in \mathrm{Ass}(I), J \subset P} P.$$

In particular, $\sqrt{(I : (I : J))} = \sqrt{(I : (I : J^\infty))}$*.*

Proof. Let $\mathcal{Q}$ be a primary decomposition of I. By Proposition 2.2.2 (2.5),

$$\sqrt{(I : (I : J^\infty))} = \bigcap_{Q \in \mathcal{Q}_2(J)} \sqrt{(Q : \bigcap_{Q' \in \mathcal{Q}_1(J)} Q')} \cap \bigcap_{Q \in \mathcal{Q}_3(J)} \sqrt{(Q : \bigcap_{Q' \in \mathcal{Q}_1(J)} Q')}.$$

Since $\mathcal{Q}$ is minimal, we obtain that $Q \not\supset \bigcap_{Q' \in \mathcal{Q}_1(J)} Q'$ for any $Q \in \mathcal{Q}_2(J)$ and $Q \not\supset \bigcap_{Q' \in \mathcal{Q}_1(J)} Q'$ for any $Q \in \mathcal{Q}_3(J)$. Thus, by Lemma 1.2.10,

$$\begin{aligned}\sqrt{(I : (I : J^\infty))} &= \bigcap_{Q \in \mathcal{Q}_2(J)} \sqrt{(Q : \bigcap_{Q' \in \mathcal{Q}_1(J)} Q')} \cap \bigcap_{Q \in \mathcal{Q}_3(J)} \sqrt{(Q : \bigcap_{Q' \in \mathcal{Q}_1(J)} Q')} \\ &= \bigcap_{Q \in \mathcal{Q}_2(J)} \sqrt{Q} \cap \bigcap_{Q \in \mathcal{Q}_3(J)} \sqrt{Q} \\ &= \bigcap_{P \in \mathrm{Ass}(I), J \subset P} P.\end{aligned}$$

From (2.2) in Proposition 2.1.2, we obtain that $\sqrt{(I : (I : J))} = \sqrt{(I : (I : J^\infty))}$. □

Example 2.2.5. *For* $I = \langle x^3y, x^2y^2 \rangle = \langle x^2 \rangle \cap \langle x^3, y^2 \rangle \cap \langle y \rangle$ *and* $J = \langle x^2 \rangle$, $\sqrt{(I : (I : J^\infty))} = \bigcap_{P \in \mathrm{Ass}(I), J \subset P} P = \langle x \rangle$.

Chapter 3

Criteria for Primary Component and Prime Divisor

In this chapter, we present several criteria for primary component which check whether a P-primary ideal Q is a primary component of I or not without computing a primary decomposition of I, based on the first saturated quotient. We first propose a general criterion applicable to any primary ideals. Then, we propose some specialized criteria aiming for isolated primary components and maximal ones. Finally, we add criteria for prime divisors. We remark that $(I : P^\infty)$ is very useful for those criteria when P is a prime divisor of I.

3.1 General Primary Component Criterion

We use the first saturated quotient to check whether a given primary ideal is a component or not. We introduce a key notion *saturated quotient invariant.*

Definition 3.1.1 ([17], Definition 24)**.** *Let I and J be ideals. We say that J is* saturated quotient invariant *with respect to I if $(I : (I : J)^\infty) = J$.*

Example 3.1.2. *Let $I = \langle x^2, xy\rangle = \langle x\rangle \cap \langle x^2, y\rangle$ and $J = \langle x\rangle$. Then J is saturated quotient invariant with respect to I since $(I : (I : J)^\infty) = (I : \langle x, y\rangle^\infty) = \langle x\rangle$.*

Here, we show that any localization of ideal is saturated quotient invariant with respect to the ideal. Conversely, any proper saturated quotient invariant ideal of I is some localization of I.

Lemma 3.1.3 ([17], Lemma 25)**.** *Let I be an ideal and J a proper ideal of $K[X]$. Then, the following conditions are equivalent.*

(A) $J = IK[X]_S \cap K[X]$ for some multiplicatively closed set S.

(B) J is saturated quotient invariant with respect to I.

Proof. Let $\mathcal{Q}$ be a primary decomposition. Show that (A) implies (B). From Proposition 2.2.2 (2.3),

$$(I : (I : IK[X]_S \cap K[X])^\infty) = \bigcap_{Q\in\mathcal{Q}, IK[X]_S\cap K[X]\subset IK[X]_{\sqrt{Q}}\cap K[X]} Q. \tag{3.1}$$

By Lemma 1.3.7, $IK[X]_S \cap K[X] \subset IK[X]_{\sqrt{Q}} \cap K[X]$ if and only if $Q \cap S = \emptyset$. Thus,

$$\bigcap_{Q \in \mathcal{Q}, IK[X]_S \cap K[X] \subset IK[X]_{\sqrt{Q}} \cap K[X]} Q = \bigcap_{Q \in \mathcal{Q}, Q \cap S = \emptyset} Q, \tag{3.2}$$

Combining (3.1), (3.2) and $IK[X]_S \cap K[X] = \bigcap_{Q \in \mathcal{Q}, Q \cap S = \emptyset} Q$ by Remark 1.1.18, we obtain that $(I : (I : IK[X]_S \cap K[X])^\infty) = IK[X]_S \cap K[X]$.

Next, show that (B) implies (A). From Proposition 2.2.2 (2.3),

$$(I : (I : J)^\infty) = \bigcap_{J \subset IK[X]_{\sqrt{Q}} \cap K[X]} Q = J. \tag{3.3}$$

Let $\mathcal{PP} = \{\sqrt{Q} \mid Q \in \mathcal{Q}, J \subset IK[X]_{\sqrt{Q}} \cap K[X]\}$. We may assume that $\mathcal{PP} \neq \emptyset$, otherwise $\mathcal{PP} = \emptyset$ and $J = K[X]$. Then $\mathcal{PP}$ is *an isolated set* (see Definition 1.1.32) since if $P' \in \mathrm{Ass}(I)$ and $P' \subset P$ for some $P \in \mathcal{PP}$, then $J \subset IK[X]_P \cap K[X] \subset IK[X]_{P'} \cap K[X]$ and $P' \in \mathcal{PP}$. Let $S = K[X] \setminus \bigcup_{P \in \mathcal{PP}} P$. By Lemma 1.2.3, $IK[X]_S \cap K[X] = \bigcap_{Q \in \mathcal{Q}, \sqrt{Q} \in \mathcal{PP}} Q = \bigcap_{J \subset IK[X]_{\sqrt{Q}} \cap K[X]} Q$. By (3.3), we obtain that $IK[X]_S \cap K[X] = J$. □

Example 3.1.4. *Let $I = \langle x^2, xy \rangle = \langle x \rangle \cap \langle x^2, y \rangle$ and $J = \langle x \rangle$. Then J is saturated quotient invariant with respect to I and $J = IK[X]_{\langle x \rangle} \cap K[X]$.*

Based on Lemma 3.1.3, we have the following criterion for primary component.

Theorem 3.1.5 (Criterion 1; [17], Theorem 26)**.** *Let I be an ideal and P a prime divisor of I. For a P-primary ideal Q, if $Q \not\supset (I : P^\infty)$, then the following conditions are equivalent.*

(A) Q is a P-primary component for some primary decomposition of I.

(B) $(I : P^\infty) \cap Q$ is saturated quotient invariant with respect to I.

Proof. Show that (A) implies (B). Let $\mathcal{Q}$ be a primary decomposition with $Q \in \mathcal{Q}$. Let $\mathcal{PP} = \{P' \in \mathrm{Ass}(I) \mid P \not\subset P' \text{ or } P' = P\}$ and $S = K[X] \setminus \bigcup_{P' \in \mathcal{PP}} P'$. Then S is a multiplicatively closed set and $(I : P^\infty) \cap Q \subset IK[X]_S \cap K[X]$ since $(I : P^\infty) \cap Q = \bigcap_{Q' \in \mathcal{Q}, P \not\subset \sqrt{Q'}} Q' \cap Q$. For each $Q' \in \mathcal{Q}$ with $Q' \cap S = \emptyset$, there is $P' \in \mathcal{PP}$ such that $\sqrt{Q'} \subset P'$, i.e. $\sqrt{Q'} \in \mathcal{PP}$. Thus, $(I : P^\infty) \cap Q \supset IK[X]_S \cap K[X]$ and $(I : P^\infty) \cap Q = IK[X]_S \cap K[X]$. By Lemma 3.1.3, $IK[X]_S \cap K[X]$ is saturated quotient invariant with respect to I.

Show that (B) implies (A). By Lemma 3.1.3, there is a multiplicatively closed set S such that $(I : P^\infty) \cap Q = IK[X]_S \cap K[X]$. Let $\mathcal{Q}$ be a primary decomposition of I. We know $IK[X]_S \cap K[X] = \bigcap_{Q' \in \mathcal{Q}, Q' \cap S = \emptyset} Q'$. By the assumption, $Q \not\supset (I : P^\infty)$ and thus $(I : P^\infty) \cap Q$ has a P-primary component. Then neither $\bigcap_{Q' \in \mathcal{Q}, Q' \cap S \neq \emptyset} Q'$ nor $(I : P^\infty)$ has a P-primary component. Hence,

$$I = (I : P^\infty) \cap Q \cap \bigcap_{Q' \in \mathcal{Q}, Q' \cap S \neq \emptyset} Q' = \bigcap_{Q' \in \mathcal{Q}, P \not\subset \sqrt{Q'}} Q' \cap Q \cap \bigcap_{Q' \in \mathcal{Q}, Q' \cap S \neq \emptyset} Q'$$

is a primary decomposition and Q is its P-primary component. □

Example 3.1.6. *Let $I = \langle x^4y + x^3y, x^2y^3 + xy^3, x^2yz, xy^2z \rangle = \langle x \rangle \cap \langle x^2, y^2 \rangle \cap \langle x^3, y^3, z \rangle \cap \langle y \rangle \cap \langle x+1, z \rangle$ and $P = \langle x, y \rangle$ in $\mathbb{Q}[x, y, z]$. Then, $(I : P^\infty) = \langle x \rangle \cap \langle y \rangle \cap \langle x + 1, z \rangle$. We think the following two P-primary ideals.*

- *$Q_1 = \langle x^2, y^2 \rangle$. Since $Q_1 \not\supset (I : P^\infty)$ and $(I : (I : ((I : P^\infty) \cap Q_1))^\infty) = (I : \langle x^3, y^3, z \rangle^\infty) = \langle x \rangle \cap \langle y \rangle \cap \langle x+1, z \rangle \cap \langle x^2, y^2 \rangle = (I : P^\infty) \cap Q_1$, we obtain that $\langle x^2, y^2 \rangle$ is a P-primary component of I.*

- $Q_2 = \langle x^2, x+y\rangle$. *Since* $(I : (I : ((I : P^\infty) \cap Q_2))^\infty) = (I : (\langle y^2, x-y\rangle \cap \langle x^3, y^3, z\rangle)^\infty) = \langle x\rangle \cap \langle y\rangle \cap \langle x+1, z\rangle \neq (I : P^\infty) \cap Q_2$, *we obtain that* $\langle x^2, x+y\rangle$ *is not a* P*-primary component of* I.

3.2 Other Criteria for Primary Component

Next, we propose criteria for primary components having special properties which can be applied for particular prime divisors. These criteria may be computed more easily than the general one.

3.2.1 Criterion for Isolated Primary Component

If Q is a primary ideal whose radical is an isolated divisor P of an ideal I, then we can use the following criterion and avoid computing $(I : P^\infty)$ since the P-primary component of I is the localization of I at P.

Theorem 3.2.1 (Criterion 2; [17], Theorem 27)**.** *Let* I *be an ideal and* P *an isolated prime divisor of* I. *For a* P*-primary ideal* Q, *the following conditions are equivalent.*

(A) Q *is the isolated* P*-primary component of* I.

(B) $(I : (I : Q)^\infty) = Q$.

Proof. Show that (A) implies (B). Let $S = K[X] \setminus P$. By Lemma 3.1.3, $Q = IK[X]_S \cap K[X]$ is saturated quotient invariant with respect to I and thus $(I : (I : Q)^\infty) = Q$. Next, we show that (B) implies (A). By Lemma 3.1.3, there is a multiplicatively closed set S s.t. $IK[X]_S \cap K[X] = Q$. Since Q is primary, $IK[X]_S \cap K[X]$ is the isolated P-primary component. □

Example 3.2.2. *For* $I = \langle x^3y, x^2y^2\rangle = \langle x^2\rangle \cap \langle x^3, y^2\rangle \cap \langle y\rangle$, *a primary component* $Q = \langle x^2\rangle$ *is isolated and* $(I : (I : Q)^\infty) = (I : (\langle x, y^2\rangle \cap \langle y\rangle)^\infty) = \langle x^2\rangle = Q$.

3.2.2 Criterion for Maximal Primary Component

Each isolated prime divisor is minimal in $\mathrm{Ass}(I)$. On the contrary, we consider "maximal prime divisor" defined below and propose the following criterion for it.

Definition 3.2.3 ([15], Definition 28)**.** *Let* P *be a prime divisor of* I. *We say that* P *is* maximal *if there is no prime divisor* P' *of* I *containing* P *properly.*

Example 3.2.4. *For* $I = \langle x^2z^2, xy^2z^2\rangle = \langle x\rangle \cap \langle x^2, y^2\rangle \cap \langle z^2\rangle$ *in* $\mathbb{Q}[x, y, z]$, *prime divisors* $P_1 = \langle x, y\rangle$ *and* $P_2 = \langle z\rangle$ *are maximal in* $\mathrm{Ass}(I) = \{\langle x\rangle, \langle x, y\rangle, \langle z\rangle\}$.

Theorem 3.2.5 (Criterion 3; [17], Theorem 29)**.** *Let* I *be an ideal and* P *a maximal prime divisor of* I. *For a* P*-primary ideal* Q, *the following conditions are equivalent.*

(A) Q *is a* P*-primary component of* I.

(B) $(I : P^\infty) \cap Q = I$.

Proof. Show that (A) implies (B). Let $\mathcal{Q}$ be a primary decomposition of I with $Q \in \mathcal{Q}$. Since P is maximal in $\mathrm{Ass}(I)$, $(I : P^\infty) = \bigcap_{Q' \in \mathcal{Q}, \sqrt{Q'} \not\supset P} Q' = \bigcap_{Q' \in \mathcal{Q}, Q' \neq Q} Q'$. Thus, $(I : P^\infty) \cap Q = \bigcap_{Q' \in \mathcal{Q}, Q' \neq Q} Q' \cap Q = I$. Next, we show that ($B$) implies ($A$). Let $\mathcal{Q}'$ be a primary decomposition of $(I : P^\infty)$. Since $\mathcal{Q}'$ does not have P-primary component, $\mathcal{Q}' \cup \{Q\}$ is a primary decomposition of I.

□

Example 3.2.6. *Let* $I = \langle x^2z^2, xy^2z^2\rangle = \langle x\rangle \cap \langle x^2, y^2\rangle \cap \langle z^2\rangle$ *and* $P = \langle x, y\rangle$ *in* $\mathbb{Q}[x, y, z]$. *Then* P *is maximal in* $\mathrm{Ass}(I)$ *and* $Q = \langle x^2, y^2\rangle$ *is a* P*-primary component of* I *since* $(I : P^\infty) \cap Q = \langle x\rangle \cap \langle z^2\rangle \cap \langle x^2, y^2\rangle = I$.

3.2.3 Criterion for Another General Primary Component

The general case can be reduced to "maximal case" via localization with respect to MIS. We recall that a subset U of X is called an MIS of I if $K[U] \cap I = \{0\}$ and the cardinality of U is equal to the dimension of I (see Definition 1.1.29). Letting $S = K[U]^\times = K[U] \setminus \{0\}$, we obtain the following as a special case of Lemma 1.2.1.

Theorem 3.2.7 (Criterion 4; [17], Theorem 30)**.** *Let* I *be an ideal and* P *a prime divisor of* I. *If* U *is an MIS of* P *and* Q *is a* P*-primary ideal , then the following conditions are equivalent.*

(A) Q *is a primary component of* I.

(B) Q *is a primary component of* $IK[X]_{K[U]^\times} \cap K[X]$.

Example 3.2.8. *For* $I = \langle x^3, xy^2, x^2z, xyz\rangle = \langle x\rangle \cap \langle x^2, y\rangle \cap \langle x^3, y^2, z\rangle$, *we obtain that* $\langle x^2, y\rangle$ *is a primary component of both* I *and* $I\mathbb{Q}[X]_{\langle x,y\rangle} \cap \mathbb{Q}[X] = \langle x\rangle \cap \langle x^2, y\rangle$.

3.3 Additional Criterion for Prime Divisor

Here, we add a criterion for prime divisor based on the third saturated quotient. The second condition (B) implies $P = (I : (I : P))$ while the third condition (C) does not always mean $P = (I : (I : P^\infty))$ (see Remark 5.1.1).

Theorem 3.3.1 (Criterion 5; [17], Theorem 31)**.** *Let* I *be an ideal and* P *a prime ideal. Then, the following conditions are equivalent.*

(A) $P \in \mathrm{Ass}(I)$.

(B) $P \supset (I : (I : P))$.

(C) $P \supset (I : (I : P^\infty))$.

Proof. By Corollary 2.1.3, (A) is equivalent to (B). By Proposition 2.2.4, $\sqrt{(I : (I : P))} = \sqrt{(I : (I : P^\infty))} = \bigcap_{P' \in \mathrm{Ass}(I), P \subset P'} P'$. Thus, the equivalence between (A) and (C) is proved by the similar way of Corollary 2.1.3. □

Example 3.3.2. *For* $I = \langle x^5 + x^4, x^3y + x^2y\rangle = \langle x^2\rangle \cap \langle x^4, y\rangle \cap \langle x + 1\rangle$ *and a prime divisor* $P = \langle x\rangle$, *it follows that* $(I : P) = \langle x\rangle \cap \langle x^3, y\rangle \cap \langle x + 1\rangle$ *and* $(I : P^\infty) = \langle x + 1\rangle$. *Thus, we obtain that* $(I : (I : P)) = \langle x\rangle \subset P$ *and* $(I : (I : P^\infty)) = \langle x^2\rangle \cap \langle x^4, y\rangle \subset P$.

Using the second saturated quotient, we can compute the *minimal pseudo-primary component* (see Proposition 1.1.22) without knowing all isolated prime divisors.

Lemma 3.3.3 ([17], Lemma 32)**.** *Let* I *be an ideal and* P *an isolated prime divisor of* I. *Then,* $(I : (I : P^\infty)^\infty)$ *is the minimal* P*-pseudo-primary component of* I.

Proof. Let $\mathcal{Q}$ be a primary decomposition of I. By Proposition 2.2.2 (2.4),

$$(I : (I : P^\infty)^\infty) = \bigcap_{Q \in \mathcal{Q}, P \subset \sqrt{IK[X]_{\sqrt{Q}} \cap K[X]}} Q.$$

Thus it is enough to show that the following statements are equivalent for each $Q \in \mathcal{Q}$.

(1-a) $P \subset \sqrt{IK[X]_{\sqrt{Q}} \cap K[X]}$.

(1-b) P is the unique isolated prime divisor which is contained in $\sqrt{Q}$.

Show that (1-a) implies (1-b). As $\sqrt{IK[X]_{\sqrt{Q}} \cap K[X]} \subset \sqrt{Q}$, we know $P \subset \sqrt{Q}$. Then, we suppose that there is another isolated prime divisor P' contained in $\sqrt{Q}$. We obtain that

$$\sqrt{IK[X]_{\sqrt{Q}} \cap K[X]} = \bigcap_{Q' \in \mathcal{Q}, Q' \subset \sqrt{Q}} \sqrt{Q'} \subset P'.$$

However, this implies $P \subset P'$ and contradicts that P' is isolated. It is easy to prove that (1-b) implies (1-a). Since P is the unique isolated prime divisor which is contained in $\sqrt{Q}$, we obtain that

$$\sqrt{IK[X]_{\sqrt{Q}} \cap K[X]} = \bigcap_{Q' \in \mathcal{Q}, Q' \subset \sqrt{Q}} \sqrt{Q'} = P.$$

□

Example 3.3.4. *For $I = \langle xy^3 + xy^2, x^2y + x^2 \rangle = \langle x \rangle \cap \langle x^2, y^2 \rangle \cap \langle y + 1 \rangle$ and $P = \langle x \rangle$, we obtain that $(I : (I : P^\infty)^\infty) = \langle x \rangle \cap \langle x^2, y^2 \rangle$ is the minimal P-pseudo-component of I.*

Using Lemma 3.3.3, we obtain the following criterion for isolated prime divisor.

Theorem 3.3.5 (Criterion 6; [17], Theorem 33)**.** *Let I be an ideal and P a prime ideal containing I. Then, the following conditions are equivalent.*

(A) P is an isolated prime divisor of I.

(B) $(I : (I : P^\infty)^\infty) \neq K[X]$.

Proof. Show that (A) implies (B). By Lemma 3.3.3, $(I : (I : P^\infty)^\infty) \neq K[X]$. Show that ($B$) implies ($A$). By Proposition 2.2.2 (2.4),

$$(I : (I : P^\infty)^\infty) = \bigcap_{Q \in \mathcal{Q}, P \subset \sqrt{IK[X]_{\sqrt{Q}} \cap K[X]}} Q \neq K[X]$$

for a primary decomposition $\mathcal{Q}$ of I. Then, there is an isolated prime divisor P' containing P. Since $\sqrt{I} \subset P \subset P'$ and P' is isolated, this implies $P = P'$ is isolated. □

Since each prime divisor of I contains I, Theorem 3.3.5 directly induces the following.

Corollary 3.3.6 (Criterion 7; [17], Corollary 34)**.** *Let I be an ideal and P a prime divisor of I. Then,*

(i) P is isolated if $(I : (I : P^\infty)^\infty) \neq K[X]$,

(ii) P is embedded if $(I : (I : P^\infty)^\infty) = K[X]$.

Example 3.3.7. *Let $I = \langle xy^3 + xy^2, x^2y + x^2 \rangle = \langle x \rangle \cap \langle x^2, y^2 \rangle \cap \langle y + 1 \rangle \subset \mathbb{Q}[x, y]$. For a prime divisor $P_1 = \langle x \rangle$, $(I : (I : P^\infty)^\infty) = \langle x \rangle \cap \langle x^2, y^2 \rangle \neq \mathbb{Q}[x, y]$ and P_1 is isolated. For a prime divisor $P_2 = \langle x, y \rangle$, $(I : (I : P^\infty)^\infty) = \mathbb{Q}[x, y]$ and P_2 is embedded.*

Chapter 4

Local Primary Algorithms

In this chapter, we devise Local Primary Algorithms (LPAs) which compute a P-primary component of I for a given prime divisor P of I. Our method applies different procedures for two cases; isolated and embedded. Algorithm 1 shows the outline of LPAs. Its termination comes from Proposition 4.1.1. When $S = K[X] \setminus P$ for an isolated prime divisor P, the P-isolated primary component of I is the effective localization of I at P.

4.1 Generating Primary Component

First, we introduce several ways to generate primary components through equidimensional hull computation.

Proposition 4.1.1 ([10], Section 4. [22], Remark 10)**.** *Let I be an ideal and P a prime divisor of I. For any positive integer m, $I + P^m$ is P-hull-primary, and for a sufficiently large integer m,* $\mathrm{hull}(I + P^m)$ *is a P-primary component appearing in a primary decomposition of I.*

Example 4.1.2. *For $I = \langle x^3, xy^2, x^2z, xyz\rangle = \langle x\rangle \cap \langle x^2, y\rangle \cap \langle x^3, y^2, z\rangle$ and $P = \langle x, y\rangle$, we obtain that*

$$I + P^3 = \langle x^3, x^2y, xy^2, y^3, x^2z, xyz\rangle$$

and $\mathrm{hull}(I+P^3) = \langle x^2, xy, y^3\rangle$ *is a P-primary component of I. Here, $I = \langle x\rangle \cap \langle x^2, xy, y^3\rangle \cap \langle x^3, y^2, z\rangle$ is another primary decomposition (see Lemma 4.2.1).*

We can use criteria for *primary component* to check if m is large enough or not. If P is an isolated prime divisor, then the P-primary component is computed directly by using the second saturated quotient. By Lemma 3.3.3, $(I : (I : P^\infty)^\infty)$ is the minimal P-pseudo-primary component of I and thus $\mathrm{hull}((I : (I : P^\infty)^\infty))$ is the isolated P-primary component of I by Lemma 1.3.5. To compute equidimensional hull, we can use *regular sequence* (see Proposition 1.4.6) or *MIS* (see Lemma 4.2.7).

Theorem 4.1.3 ([17], Theorem 36)**.** *Let I be an ideal and P an isolated prime divisor of I. Then*

$$\mathrm{hull}((I : (I : P^\infty)^\infty))$$

is the isolated P-primary component of I.

Example 4.1.4. *For* $I = \langle x^2y^3+x^2y^2, x^3y+x^3\rangle = \langle x^2\rangle \cap \langle x^3, y^2\rangle \cap \langle y+1\rangle$ *and* $P = \langle x\rangle$*, the isolated* P*-primary component is* $\mathrm{hull}((I : (I : P^\infty)^\infty)) = \mathrm{hull}(\langle x^3, x^2y^2\rangle)$*. Here,* x^3 *is a regular sequence of* $\langle x^3, x^2y^2\rangle = \langle x^2\rangle \cap \langle x^3, y^2\rangle$ *and the codimension of* $\langle x^2\rangle \cap \langle x^3, y^2\rangle$ *is* 1*. Thus* $\mathrm{hull}(\langle x^3, x^2y^2\rangle) = (\langle x^3\rangle : (\langle x^3\rangle : (\langle x^3, x^2y^2\rangle))) = (\langle x^3\rangle : \langle x\rangle) = \langle x^2\rangle$ *by Proposition 1.4.6*

Algorithm 1 General Frame of Local Primary Algorithm

Input: I: an ideal, P: a prime ideal

Output: • a P-primary component of I if P is a prime divisor of I
• "P is not a prime divisor" otherwise

if P is a prime divisor of I (**Criterion 5**) **then**
  if P is isolated (**Criteria 6,7**) **then**
    $\overline{Q} \leftarrow$ the minimal P-pseudo-primary component of I (**Lemma 3.3.3**)
    $Q \leftarrow \mathrm{hull}(\overline{Q})$ (**Theorem 4.1.3**)
    return Q is the isolated P primary component
  else
    $m \leftarrow 1$, $Q \leftarrow K[X]$
    while Q is not primary component of I (**Criteria 1,3,4**) **do**
      $\overline{Q} \leftarrow$ a P-hull-primary ideal related to m (**Proposition 4.1.1, Lemma 4.2.3**)
      $Q \leftarrow \mathrm{hull}(\overline{Q})$
      $m \leftarrow m + 1$
    end while
    return Q is an embedded P-primary component
  end if
else
  return "P is not a prime divisor"
end if

4.2 Techniques for Improving LPAs

We introduce practical techniques for implementing LPAs.

4.2.1 Another Way of Generating Primary Component

Let $G = \{f_1, \ldots, f_r\}$ be a generator of a prime ideal P. Usually we take $\{f_1^{e_1}f_2^{e_2}\cdots f_r^{e_r} \mid e_1+\cdots+e_r = m\}$ as a generator of P^m for a positive integer m. However, this generator has $\frac{(r+m-1)!}{(r-1)!m!}$ elements and it becomes difficult to compute $\mathrm{hull}(I+P^m)$ when m becomes large. To avoid the explosion of the number of the generator, we can use $P_G^{[m]} = \langle f_1^m, \ldots, f_r^m\rangle$ instead.

First, we introduce a lemma to compute primary decomposition by using equdimensional hull.

Lemma 4.2.1 ([17], Lemma 37)**.** *Let* $\mathcal{Q}$ *be a primary decomposition of* I *and* $Q \in \mathcal{Q}$*. If* $\sqrt{Q}$*-hull-primary ideal* Q' *satisfies* $I \subset Q' \subset Q$*, then* $(\mathcal{Q}\setminus\{Q\})\cup\{\mathrm{hull}(Q')\}$ *is another primary decomposition of* I*.*

Proof. By Lemma 1.3.9, we obtain that $I \subset Q' \subset \mathrm{hull}(Q') \subset Q$. Since $I \cap \mathrm{hull}(Q') = I$ and

$Q \cap \mathrm{hull}(Q') = \mathrm{hull}(Q')$, we obtain that

$$I = I \cap \mathrm{hull}(Q') = \left(\bigcap_{Q'' \in \mathcal{Q}, Q'' \neq Q} Q'' \cap Q \right) \cap \mathrm{hull}(Q') = \bigcap_{Q'' \in \mathcal{Q}, Q'' \neq Q} Q'' \cap \mathrm{hull}(Q').$$

Thus, $(\mathcal{Q} \setminus \{Q\}) \cup \{\mathrm{hull}(Q')\}$ is an irredundant primary decomposition of I. □

Example 4.2.2. *Let $I = \langle x^2z, xyz \rangle = \langle x \rangle \cap \langle x^2, y \rangle \cap \langle z \rangle$, $Q' = \langle y^3, y^2z + y^2, x^2, xy \rangle = \langle x^2, xy, y^2 \rangle \cap \langle x^2, xy, y^3, z+1 \rangle$ and $P = \langle x, y \rangle$. Then, Q' is P-hull-primary. For a primary component $Q = \langle x^2, y \rangle$, we obtain that $I \subset Q' \subset Q$ and $\mathrm{hull}(Q') = \langle x^2, xy, y^2 \rangle$ is also a P-primary component of I.*

Next, the following lemma gives another efficient way to compute a primary component from its prime divisor.

Lemma 4.2.3 ([17], Lemma 38)**.** *For any positive integer m, $I + P_G^{[m]}$ is P-hull-primary, and for a sufficiently large integer m, $\mathrm{hull}(I + P_G^{[m]})$ is a P-primary component appearing in a primary decomposition of I if P is a prime divisor of I.*

Proof. As $\sqrt{P_G^{[m]}} = P$ and $\sqrt{I + P} = \sqrt{I + P_G^{[m]}} = P$, $I + P_G^{[m]}$ is P-hull-primary. By Proposition 4.1.1, $\mathrm{hull}(I + P^m)$ is a P-primary component of I for a sufficiently large integer m. Since $I \subset I + P_G^{[m]} \subset I + P^m \subset \mathrm{hull}(I + P^m)$, $\mathrm{hull}(I + P_G^{[m]})$ is a P-primary component by Lemma 4.2.1. □

Example 4.2.4. *For $I = \langle x^3, xy^2, x^2z, xyz \rangle = \langle x \rangle \cap \langle x^2, y \rangle \cap \langle x^3, y^2, z \rangle$ and $P = \langle G \rangle = \langle x, y \rangle$, we obtain that $I + P_G^{[3]} = \langle x^3, xy^2, y^3, x^2z, xyz \rangle$ and $\mathrm{hull}(I + P_G^{[3]}) = \langle x^2, xy, y^3 \rangle$ is a P-primary component of I.*

4.2.2 Regular Sequence Computation for Pseudo-Primary Ideal

We can compute a regular sequence in a P-pseudo-primary ideal I from one of P by the following lemma. Since a generator of P may be more easily than one of I, it tends to be less time-consuming.

Lemma 4.2.5 ([18], Lemma 56)**.** *Let I be a P-pseudo-primary ideal and $f_1, \ldots, f_c$ a regular sequence in P. Then, for sufficiently large integers $m_1, \ldots, m_c$, $f_1^{m_1}, \ldots, f_c^{m_c}$ is a regular sequence in I.*

Proof. By Theorem 26 in [21], $f_1^{m_1}, \ldots, f_c^{m_c}$ is a regular sequence for any positive integers $m_1, \ldots, m_c$. Since I is P-pseudo-primary, it follows that $\sqrt{I} = P$. Thus, for sufficiently large integers $m_1, \ldots, m_c$, $\{f_1^{m_1}, \ldots, f_c^{m_c}\} \subset I$ and $f_1^{m_1}, \ldots, f_c^{m_c}$ is a regular sequence in I. □

Since $\sqrt{(I : (I : P^\infty)^\infty)} = P$ if P is isolated, we obtain the following corollary. From $\mathrm{codim}(P) = \mathrm{codim}((I : (I : P^\infty)^\infty))$ and Lemma 1.4.6, we can compute the *equidimensional hull* $\mathrm{hull}((I : (I : P^\infty)^\infty))$ by using a regular sequence in P.

Corollary 4.2.6 ([18], Corollary 57)**.** *Let I be an ideal and P its isolated prime divisor. Let $f_1, \ldots, f_c$ be a regular sequence in P. Then, for a sufficiently large integer m, $f_1^{m_1}, \ldots, f_c^{m_c}$ is a regular sequence in $(I : (I : P^\infty)^\infty)$.*

4.2.3 Equidimensional Hull Computation with MIS

Next, we devise another computation of $\mathrm{hull}(I+P^m)$ based on MIS which tends to be much efficient than computations based on Proposition 1.4.6. Similarly, by this technique we can replace I with $IK[X]_{K[U]^\times} \cap K[X]$ for an MIS U of P at the first step of LPA.

Lemma 4.2.7 ([17], Lemma 39)**.** *Let I be a P-hull-primary ideal. For an MIS U of P,* $\mathrm{hull}(I) = IK[X]_{K[U]^\times} \cap K[X]$.

Proof. Let $\mathcal{Q}$ be a primary decomposition of I. Then, $\mathrm{hull}(I)$ is the unique primary component disjoint from $K[U]^\times$. Thus, $IK[X]_{K[U]^\times} \cap K[X] = \bigcap_{Q\in\mathcal{Q}, Q\cap K[U]^\times=\emptyset} Q = \mathrm{hull}(I)$. □

Example 4.2.8. *For $I = \langle x^2, xy\rangle = \langle x\rangle \cap \langle x^2, y\rangle$ and $P = \langle x\rangle$ in $\mathbb{Q}[X] = \mathbb{Q}[x, y]$, we obtain that I is P-hull-primary and $U = \{y\}$ is an MIS of P. Then,* $\mathrm{hull}(I) = \langle x\rangle = I\mathbb{Q}[X]_{\mathbb{Q}[U]^\times} \cap \mathbb{Q}[X]$.

4.3 Further Discussion of LPAs

In this section, we devise another algorithm "LPA-($P_G^{[m]}$+MIS) without DIQ" to compute the particular primary component, without DIQ and its variants. The algorithm uses equidimensional hull to generate primary component in the similar way as LPAs. As different points, it uses MIS for another criterion of prime divisors and a generalized splitting tool for an additional criterion of primary components.

First, we introduce a new criterion for prime divisors using MIS instead of DIQ.

Proposition 4.3.1 (Criterion 8; [18], Proposition 60)**.** *Let I be an ideal and P a prime ideal in $K[X]$. Then the following conditions are equivalent.*

(1) $P \in \mathrm{Ass}(I)$.

(2) $(I' : P^\infty) \neq I'$, *where $I' = IK[X]_{K[U]^\times} \cap K[X]$ for an MIS U of P.*

Proof. Let $\mathcal{Q}$ be a primary decomposition of I. To prove that (1) implies (2), we remark that $P \in \mathrm{Ass}(I)$ leads $P \in \mathrm{Ass}(I')$ from Lemma 1.2.1 and $P \cap K[U]^\times = \emptyset$. Thus, we obtain that $(I' : P^\infty) \neq I'$ since $P \notin \mathrm{Ass}((I' : P^\infty))$. Next, we show that (2) implies (1). Since $(I' : P^\infty) \neq I'$, there is a prime divisor $P' \in \mathrm{Ass}(I')$ containing P. Then $P' \cap K[U]^\times = \emptyset$ and $\dim(P') \leq \dim(P) = \#U$. From Lemma 1.2.1, $P' \in \mathrm{Ass}(I)$ and thus $\dim(P') \geq \#U$. Hence, $\dim(P) = \dim(P')$ and $P = P' \in \mathrm{Ass}(I)$. □

Example 4.3.2. *Let $I = \langle x^3, x^2y\rangle = \langle x^2\rangle \cap \langle x^3, y\rangle$ and $P = \langle x\rangle$ in $\mathbb{Q}[X] = \mathbb{Q}[x, y]$. Then, $U = \{y\}$ is the MIS of P and $I' = I\mathbb{Q}[X]_{\mathbb{Q}[U]^\times} \cap \mathbb{Q}[X] = \langle x^2\rangle$. Since $(I' : P^\infty) = \mathbb{Q}[X] \neq I'$, we conclude $P \in \mathrm{Ass}(I)$.*

Next, we introduce a *P-pseudo-descending chain* to devise a generalized splitting tool and a new criterion for isolated prime divisors. It is a generalization of P^m and $P_G^{[m]}$.

Definition 4.3.3 (P-pseudo-descending chain; [18], Definition 62)**.** *Let P be a prime ideal and $J_1 \supset J_2 \supset J_3 \supset \cdots$ a descending chain of P-pseudo-primary ideals. We say that $J_1 \supset J_2 \supset J_3 \supset \cdots$ is a* P-pseudo-descending chain *if $PJ_m \supset J_{m+1}$ for every positive integer m.*

Example 4.3.4. *As an easy example, $P \supset P^2 \supset P^3 \supset \cdots$ is a P-pseudo-descending chain. For a generator G of P, $P_G^{[1]} \supset P_G^{[2]} \supset P_G^{[3]} \supset \cdots$ is a P-pseudo-descending chain since $P_G^{[m]}$ is P-pseudo-primary and $PP_G^{[m]} \supset P_G^{[m+1]}$ for every m.*

Remark 4.3.5. *We remark that a P-pseudo-descending chain is not always a P-filtration i.e. it does not always satisfy the other inclusion $PJ_m \subset J_{m+1}$.*

We can use a P-pseudo-descending chain to generate a P-primary component as Lemma 4.3.6, a generalization of Proposition 4.1.1 and Lemma 4.2.3.

Lemma 4.3.6 ([18], Lemma 65)**.** *Let I be an ideal, P a prime divisor of I and $J_1 \supset J_2 \supset J_3 \supset \cdots$ be a P-pseudo-descending chain. Then, for a sufficiently integer m,* $\mathrm{hull}(I + J_m)$ *is a P-primary component of I. Moreover, if* $\mathrm{hull}(I + J_m)$ *is a P-primary component of I for some m, then* $\mathrm{hull}(I + J_{m+1})$ *is also a P-primary component of I.*

Proof. Let Q be a P-primary component of I. Since $K[X]$ is Noetherian, there is a sufficiently large integer m s.t. $P^m \subset Q$. As $P^m \supset P^{m-1}J_1 \supset P^{m-2}J_2 \supset \cdots \supset PJ_{m-1} \supset J_m$, it follows that $I \subset I + J_m \subset Q$. Here, $\sqrt{I + J_m} = \sqrt{\sqrt{I} + P} = P$ and thus $I + J_m$ is P-pseudo-primary, in particular, P-hull-primary. From Lemma 4.2.1, we obtain that $\mathrm{hull}(I + J_m)$ is a P-primary component of I. Next, we show the second statement. If $\mathrm{hull}(I + J_m)$ is a P-primary component of I for some m, then it follows that $I \subset I + J_{m+1} \subset I + J_m \subset \mathrm{hull}(I + J_m)$. Thus, $\mathrm{hull}(I + J_{m+1})$ is a P-primary component of I from Lemma 4.2.1. □

Example 4.3.7. *Let $I = \langle x^2, xy\rangle = \langle x\rangle \cap \langle x^2, y\rangle$, $P = \langle x, y\rangle$ and $J_m = \langle x^m, y^m\rangle$. We obtain that* $\mathrm{hull}(I + J_m) = \langle x^2, xy, y^m\rangle$ *is a P-primary component of I if $m \geq 2$.*

Here, we devise a generalized splitting tool and find an integer m s.t. $\mathrm{hull}(I+J_m)$ is a P-primary component as follows.

Proposition 4.3.8 (Generalized Splitting Tool; [18], Proposition 67)**.** *Let I be an ideal, P a prime divisor of I and $J_1 \supset J_2 \supset J_3 \supset \cdots$ be a P-pseudo-descending chain. Then, for a sufficiently large integer m,*

$$I = (I : P^\infty) \cap (I + J_m).$$

In particular, for such m, $\mathrm{hull}(I + J_m)$ *is a P-primary component of I.*

Proof. By Lemma 1.2.7, $I = (I : P^\infty) \cap (I + P^m)$ for a sufficiently large integer m. As $J_m \subset P^m$, it follows that

$$I = (I : P^\infty) \cap (I + P^m) \supset (I : P^\infty) \cap (I + J_m) \supset I$$

and thus $I = (I : P^\infty) \cap (I + J_m)$. Since $(I : P^\infty)$ does not have a P-primary component and $I + J_m$ is P-hull-primary, we obtain that $\mathrm{hull}(I + J_m)$ is a P-primary component of I. □

Example 4.3.9. *Let $I = \langle x^2, xy\rangle = \langle x\rangle \cap \langle x^2, y\rangle$, $P = \langle x, y\rangle$ and $J_m = \langle x^m, y^m\rangle$. We obtain that $I = (I : P^\infty) \cap (I + J_2) = \langle x\rangle \cap \langle x^2, xy, y^2\rangle$ and $\langle x^2, xy, y^2\rangle$ is a P-primary component of I.*

A P-pseudo-descending chain gives us the following criteria for isolated prime divisors.

Theorem 4.3.10 (Criterion 9; [18], Theorem 69)**.** *Let I be an ideal, P a prime divisor of I and $J_1 \supset J_2 \supset J_3 \supset \cdots$ a P-pseudo-descending chain. We suppose that* $\mathrm{hull}(I + J_m)$ *is a P-primary component of I for some m. Then, the following statements are equivalent.*

(1) P is an isolated prime divisor of I.

(2) $\mathrm{hull}(I + J_m) = \mathrm{hull}(I + J_{m+1})$.

Proof. First, we show that (1) implies (2). By Lemma 4.3.6, $\mathrm{hull}(I + J_{m+1})$ is also a P-primary component of I. Since P is isolated, the P-primary component is determined independently from the choice of primary decompositions and $\mathrm{hull}(I + J_m) = \mathrm{hull}(I + J_{m+1})$. Second, we show that (2) implies (1). Let $R = K[X]_P/IK[X]_P$. Since $I+J_m$ is P-hull-primary, it follows that $\mathrm{hull}(I+J_m) = (I + J_m)K[X]_P \cap K[X]$ and thus $\mathrm{hull}(I + J_m)R = J_mR$. As $\mathrm{hull}(I + J_m) = \mathrm{hull}(I + J_{m+1})$, we obtain that $J_mR = J_{m+1}R$. Thus, from $J_m \supset PJ_m \supset J_{m+1}$, it follows that $J_mR \supset PJ_mR \supset J_{m+1}R = J_mR$, hence, $J_mR = PJ_mR$. Since J_mR is a finitely generated $K[X]_P$-module, we obtain that $J_mR = 0$ by Nakayama's Lemma (see Lemma 2.1.30 in [13]). Thus, $J_mK[X]_P = IK[X]_P$ and $P \in \mathrm{Ass}(\sqrt{I})$, otherwise, $IK[X]_P$ has two or more prime divisors. Therefore, P is isolated. □

Example 4.3.11. *Let $I = \langle x^3, x^2y\rangle = \langle x^2\rangle \cap \langle x^3, y\rangle$. For $P_1 = \langle x\rangle$, it follows that* $\mathrm{hull}(I + P_1^2) = \mathrm{hull}(I + P_1^3) = \langle x^2\rangle$ *is a P_1-primary component. Thus, P_1 is the isolated prime divisor of I. On the other hand, for $P_2 = \langle x, y\rangle$ and $J_m = \langle x^m, y^m\rangle$,* $\mathrm{hull}(I + J_3) = \langle x^3, x^2y, y^3\rangle$ *is a P_2-primary component and hull$(I + J_3) \supsetneq$* $\mathrm{hull}(I + J_4) = \langle x^3, x^2y, y^4\rangle$*; thus P_2 is embedded.*

Remark 4.3.12. *An integer m s.t.* $\mathrm{hull}(I+J_m)$ *is a P-primary component of I may be smaller than m' s.t.* $\mathrm{hull}(I + P^{m'})$ *is a P-primary component of I. Thus, by taking $J_m = P_G^{[m]}$, we may compute a primary component more easily by* $\mathrm{hull}(I + P_G^{[m]})$*. It is worth to think $P_G^v = \langle f_1^{m_1}, \ldots, f_r^{m_r}\rangle$ for a vector $v = (m_1, \ldots, m_r) \in \mathbb{Z}^r_{\geq 0}$ for an efficient computation of a primary component by* $\mathrm{hull}(I+P_G^v)$.

Algorithm 2 is another version of Local Primary Algorithm, without using DIQ. As J_m, we use $P_G^{[m]}$ (currently we think this J_m is the best), for efficient computations, and an MIS in steps of the following algorithm.

Algorithm 2 Local Primary Algorithm Without Double Ideal Quotient

Input: I: an ideal, P: a prime ideal in $K[X]$

Output: • a P-primary component if P is a prime divisor
• "P is not a prime divisor" otherwise

1: $U \leftarrow$ a Maximal Independent Set of P, $I' \leftarrow IK[X]_{K[U]^\times} \cap K[X]$
2: $G \leftarrow \{f_1, \ldots, f_s\}$ a generator of P, $m \leftarrow 1$
3: **if** $(I' : P^\infty) = I'$ **then**
4: **return** "P is not a prime divisor " (**Criterion 8**)
5: **end if**
6: **while** $(I' : P^\infty) \cap (I' + P_G^{[m]}) \neq I'$ **do**
7: $m \leftarrow m + 1$ (**Proposition 4.3.8**)
8: **end while**
9: $Q_m \leftarrow \mathrm{hull}(I' + P_G^{[m]}) = (I' + P_G^{[m]})K[X]_{K[U]^\times} \cap K[X]$ (**Lemma 4.2.7**)
10: $Q_{m+1} \leftarrow \mathrm{hull}(I' + P_G^{[m+1]}) = (I' + P_G^{[m+1]})K[X]_{K[U]^\times} \cap K[X]$
11: **if** $Q_m = Q_{m+1}$ **then**
12: **return** "Q_m is the isolated P-primary component of I " (**Criterion 9**)
13: **else**
14: **return** "Q_m is an embedded P-primary component of I " (**Criterion 9**)
15: **end if**

Remark 4.3.13. *When we compute all primary components $Q_1, \ldots, Q_r$ of I by LPAs from a given* $\mathrm{Ass}(I) = \{P_1, \ldots, P_r\}$*, the intersection of $Q_1, \ldots, Q_r$ coincides with I. We independently prove this by mathematical induction on the number of primary components r. When $r = 1$, there is nothing to show. Suppose $r > 1$. We may assume $P = \sqrt{Q_r}$ is a maximal prime divisor of I (see Definition 3.2.3). Then, Q_i is a primary component of $(I : P^\infty)$ for $i < r$ by Lemma 1.2.1 since $(I : P^\infty)$ is the localization of I with respect to $S = K[X] \setminus \bigcup_{i=1}^{r-1} \sqrt{Q_i}$. Thus, by the assumption of the induction, $\bigcap_{i=1}^{r-1} Q_i = (I : P^\infty)$. Here, by Theorem 3.2.5, $(I : P^\infty) \cap Q_r = I$. Hence, We obtain that $\bigcap_{i=1}^{r} Q_i = \bigcap_{i=1}^{r-1} Q_i \cap Q_r = (I : P^\infty) \cap Q_r = I$.*

Chapter 5

Modular Methods for Effective Localization

In this chapter, we introduce modular techniques for (double) ideal quotient and saturation. It is well-known that modular techniques are useful to avoid *intermediate coefficient growth* and have a good relationship with parallel computing. To apply modular techniques, we devise some generalizations of criteria for prime divisors and primary components presented in Chapter 3.

5.1 Generalizations of Criteria by DIQs

In this section, we introduce some generalizations of criteria for prime divisors and primary components by DIQs. First, the following remark is important to devise *modular associated test* (Theorem 5.2.9).

Remark 5.1.1. *In Theorem 3.3.1, the condition $P \supset (I : (I : P))$ is equivalent to $P = (I : (I : P))$ since $P \subset (I : (I : P))$ always holds for any ideals I and P. Indeed, $P(I : P) \subset I$ from the definition of $(I : P)$ and thus $P \subset (I : (I : P))$.*

Next, we remark some relationships between DIQ and localizations as follows.

Remark 5.1.2. *The operations of DIQ and localization at a prime ideal are commutative. Indeed, for ideals I, J and a prime ideal P, $(I : J)_P = (I_P : J_P)$ from Corollary 3.15 in [1] and thus we obtain that $(I : (I : J))_P = (I_P : (I : J)_P) = (I_P : (I_P : J_P))$. Similarly, we have $(I : (I : J^\infty))_P = (I_P : (I : J^\infty)_P) = (I_P : (I_P : J_P^\infty))$ as $(I : J^\infty) = (I : J^m)$ and $(I_P : J_P^\infty) = (I_P : J_P^m)$ for a sufficiently large integer m. Also, a prime ideal P is associated with an ideal I if and only if P_P is associated with I_P since there is a correspondence between primary decompositions of I and I_P (see Proposition 4.9 in [1]). Similarly, for a P-primary ideal Q, Q is a P-primary component of I if and only if Q_P is a P_P-primary component of I_P.*

Next, we introduce extended theorems about DIQ and its variants toward *intermediate primary decomposition* in Section 5.3. Theorem 3.3.1 gives a relationship between an ideal I and a prime divisor P. It can be extended to one between an ideal I and an intersection of some prime divisors J. Thus, we consider a radical ideal J instead of a prime ideal P as follows.

Theorem 5.1.3 ([15], Theorem 2.1.4)**.** *Let I be an ideal and J a proper radical ideal. Then, the following conditions are equivalent.*

(A) $\mathrm{Ass}(J) \subset \mathrm{Ass}(I)$,
(B) $J \supset (I : (I : J))$,
(C) $J \supset (I : (I : J^{\infty}))$.

Proof. First, we show that (A) implies (B). Let $P \in \mathrm{Ass}(J) \subset \mathrm{Ass}(I)$. Then, $P \supset (I : (I : P))$ by Theorem 3.3.1. Thus, $P \supset (I : (I : P)) \supset (I : (I : J))$. Since $J = \bigcap_{P \in \mathrm{Ass}(J)} P$, we obtain that $J \supset (I : (I : J))$. Next, we show that (B) implies (C). As $(I : J) \subset (I : J^{\infty})$, we obtain that $J \supset (I : (I : J)) \supset (I : (I : J^{\infty}))$. Finally, we show that (C) implies (A). Let $P \in \mathrm{Ass}(J)$. Then, $J_P \supset (I : (I : J^{\infty}))_P = (I_P : (I_P : J_P^{\infty}))$ from Remark 5.1.2 and thus $J_P = P_P \in \mathrm{Ass}(I_P)$ from Theorem 3.3.1. Hence, $P \in \mathrm{Ass}(I)$ by Remark 5.1.2. □

Example 5.1.4. *Let $I = \langle x^5+x^3, x^3y+xy \rangle = \langle x \rangle \cap \langle x^3, y \rangle \cap \langle x^2+1 \rangle \subset \mathbb{Q}[x, y]$ and $J = \langle x, y \rangle \cap \langle x^2+1 \rangle$. Then, $(I : (I : J)) = \langle x, y \rangle \cap \langle x^2+1 \rangle = J$ and $\mathrm{Ass}(J) = \{\langle x, y \rangle, \langle x^2+1 \rangle\} \subset \mathrm{Ass}(I) = \{\langle x \rangle, \langle x, y \rangle, \langle x^2+1 \rangle\}$. In addition, we obtain that $(I : (I : J^{\infty})) = \langle x^2, y \rangle \cap \langle x^2+1 \rangle \subset J$.*

Here, we generalize Proposition 4.1.1 to an intersection of equidimensional prime divisors as follows.

Lemma 5.1.5 ([15], Lemma 2.1.7)**.** *Let I be an ideal and J an intersection of prime divisors of I. Suppose J is unmixed i.e. $\dim(P) = \dim(J)$ for any $P \in \mathrm{Ass}(J)$. Then, for a sufficiently large integer m, $\mathrm{hull}(I + J^m)$ is an intersection of primary components appearing in a primary decomposition of I i.e. $\mathrm{hull}(I + J^m) = \bigcap_{P \in \mathrm{Ass}(J)} Q(P)$ where $Q(P)$ is a P-primary component of I.*

Proof. Let m be a positive integer. First, we note that, for each $P \in \mathrm{Ass}(J)$, $I \subset \mathrm{hull}(I + J^m)_P \cap K[X] \subset \mathrm{hull}(I + P^m)$ since

$$\begin{aligned} I \subset I + J^m \subset \mathrm{hull}(I + J^m) \subset \mathrm{hull}(I + J^m)_P \cap K[X] \\ \subset \mathrm{hull}(I + P^m)_P \cap K[X] = \mathrm{hull}(I + P^m) \end{aligned}$$

where the last equality comes from the fact that $\sqrt{I + P^m} = P$ and P is the unique isolated prime divisor of $I + P^m$. By Lemma 4.1.1, there exist a sufficiently large integer $m(P)$ and a primary decomposition $\mathcal{Q}$ of I such that $\mathrm{hull}(I + P^{m(P)}) \in \mathcal{Q}$. Then,

$$I \subset \bigcap_{P \in \mathrm{Ass}(J)} \mathrm{hull}(I + J^{m(P)})_P \cap K[X] \subset \bigcap_{P \in \mathrm{Ass}(J)} \mathrm{hull}(I + P^{m(P)})$$

and, by intersecting $\bigcap_{Q \in \mathcal{Q}, \sqrt{Q} \notin \mathrm{Ass}(J)} Q$ with them, we obtain that

$$\begin{aligned} I &\subset \left(\bigcap_{P \in \mathrm{Ass}(J)} \mathrm{hull}(I + J^{m(P)})_P \cap K[X] \right) \cap \bigcap_{Q \in \mathcal{Q}, \sqrt{Q} \notin \mathrm{Ass}(J)} Q \\ &\subset \left(\left(\bigcap_{P \in \mathrm{Ass}(J)} \mathrm{hull}(I + P^{m(P)}) \right) \cap \bigcap_{Q \in \mathcal{Q}, \sqrt{Q} \notin \mathrm{Ass}(J)} Q = I. \right. \end{aligned}$$

Thus, $\left(\bigcap_{P\in \mathrm{Ass}(J)} \mathrm{hull}(I+J^{m(P)})_P \cap K[X]\right) \cap \bigcap_{Q\in\mathcal{Q},\sqrt{Q}\notin \mathrm{Ass}(J)} Q = I$ and $\mathrm{hull}(I+J^{m(P)})_P \cap K[X]$ is a P-primary component of I. Since J is unmixed, $\sqrt{I+J^m} = \sqrt{J} = \bigcap_{P\in\mathrm{Ass}(J)} P$ and $\mathrm{Ass}(\mathrm{hull}(I+J^m)) = \mathrm{Ass}(J)$ i.e. $\mathrm{hull}(I+J^m) = \bigcap_{P\in\mathrm{Ass}(J)} \mathrm{hull}(I+J^m)_P \cap K[X]$. Thus, for $m \geq \max\{m(P) \mid P \in \mathrm{Ass}(J)\}$, $\mathrm{hull}(I+J^m)$ is an intersection of primary components of a primary decomposition of I. □

We also generalize Theorem 3.1.5 to an intersection of primary components as follows. We can check whether m appearing in Lemma 5.1.5 is large enough or not by Theorem 5.1.6. We remark that Theorem 3.1.5 holds for any Noetherian rings.

Theorem 5.1.6 ([15], Theorem 2.1.9)**.** *Let I be an ideal and J an intersection of prime divisors of I. Suppose J is unmixed. For an unmixed ideal L with $\sqrt{L} = J$, assume that $\sqrt{(L : (I : J^\infty))} = J$ and let $Z = (I : J^\infty) \cap L$. Then, the following conditions are equivalent.*

(A) $L = \bigcap_{P\in\mathrm{Ass}(J)} Q(P)$ *where $Q(P)$ is a P-primary components of I.*

(B) $(I : (I : Z)^\infty) = Z$.

Proof. First, we show that (A) implies (B). From (A), it is easy to see that $\mathcal{T} = \mathrm{Ass}((I : J^\infty)) \cup \mathrm{Ass}(L)$ is *an isolated set* (see Definition 1.1.32). Indeed, for $P' \in \mathrm{Ass}(I)$, if there exists $P \in \mathcal{T}$ s.t. $P' \subset P$, then $P' \in \mathcal{T}$ since $\mathrm{Ass}((I : J^\infty)) = \{P'' \in \mathrm{Ass}(I) \mid J \not\subset P''\}$ (see Lemma 1.2.10 (1.4)) and $\mathrm{Ass}(L) = \mathrm{Ass}(J)$. Thus, for $S = K[X] \setminus (\bigcup_{P\in\mathcal{T}} P)$, we obtain that $Z = IK[X]_S \cap K[X]$ from Lemma 1.2.3 and $\mathcal{T} = \mathrm{Ass}(Z)$. By Lemma 3.1.3, we obtain that $(I : (I : Z)^\infty) = Z$.

Second, we show that (B) implies (A). Let $P \in \mathrm{Ass}(J)$. Then, we obtain that $P_P = J_P$ and $\sqrt{L_P} = (\sqrt{L})_P = J_P = P_P$. Thus, L_P is a P_P-primary ideal and $Z_P = (I : J^\infty)_P \cap L_P = (I_P : J_P^\infty) \cap L_P$. Since $\sqrt{(L : (I : J^\infty))} = J$, $\sqrt{(L_P : (I_P : J_P^\infty))} = P_P$ and thus $L_P \not\supset (I_P : J_P^\infty)$; otherwise we get $\sqrt{(L_P : (I_P : J_P^\infty))} = K[X]_P \neq P_P$. Here, $(I_P : (I_P : Z_P)^\infty) = Z_P$ for all $P \in \mathrm{Ass}(J)$ since $(I : (I : Z)^\infty) = Z$ and $(I_P : (I_P : Z_P)^\infty) = (I : (I : Z)^\infty)_P$. Thus, by Theorem 3.1.5, L_P is a primary component of I_P. Since L is unmixed and $L = \sqrt{J}$, it follows that $L = \bigcap_{P\in\mathrm{Ass}(J)} L_P \cap K[X]$. From Remark 5.1.2, $L_P \cap K[X]$ is a P-primary component of I if and only if L_P is a P_P-primary component of I_P. Finally, we obtain the equivalence. □

We generalize Theorem 4.1.3 as follows. We remark that each $Q(P)$ in the following theorem is determined uniquely since it is an isolated primary component of I.

Theorem 5.1.7 ([15], Theorem 2.1.11)**.** *Let I be an ideal and J an intersection of isolated prime divisors of I. Suppose J is unmixed. Then*

$$\mathrm{hull}((I : (I : J^\infty)^\infty)) = \bigcap_{P\in\mathrm{Ass}(J)} Q(P)$$

where $Q(P)$ is the isolated P-primary component of I.

Proof. Let $\mathcal{Q}$ be a primary decomposition of I. By Proposition 2.2.2 (2.4), we obtain that

$$(I : (I : J^\infty)^\infty) = \bigcap_{Q\in\mathcal{Q}, J\subset\sqrt{IK[X]_{\sqrt{Q}}\cap K[X]}} Q.$$

Since $J \subset \sqrt{IK[X]_{\sqrt{Q(P)}} \cap K[X]} = \sqrt{Q(P)} = P$ for $P \in \mathrm{Ass}(J) \subset \mathrm{Ass}_{iso}(I)$, it follows that

$$(I : (I : J^\infty)^\infty) = \bigcap_{P \in \mathrm{Ass}(J)} Q(P) \cap \bigcap_{Q \in \mathcal{Q}, J \subset \sqrt{IK[X]_{\sqrt{Q}} \cap K[X]}, \sqrt{Q} \notin \mathrm{Ass}(J)} Q.$$

As J is unmixed, each $Q(P)$ has the same dimension for $P \in \mathrm{Ass}(J)$. Then,

$$\dim(\bigcap_{Q \in \mathcal{Q}, J \subset \sqrt{IK[X]_{\sqrt{Q}} \cap K[X]}, \sqrt{Q} \notin \mathrm{Ass}(J)} Q) < \dim(J)$$

from the fact that for $Q \in \mathcal{Q}$ with $J \subset \sqrt{IK[X]_{\sqrt{Q}} \cap K[X]}$ and $\sqrt{Q} \notin \mathrm{Ass}(J)$, there exists $P \in \mathrm{Ass}(J)$ s.t. $P \subsetneq \sqrt{Q}$. Since J is an intersection of isolated prime divisors of I, we obtain that

$$\mathrm{hull}((I : (I : J^\infty)^\infty)) = \bigcap_{P \in \mathrm{Ass}(J)} Q(P).$$

□

5.2 Modular Techniques for DIQ

We propose modular techniques for DIQ. For a prime number p, let $\mathbb{Z}_{(p)} = \{a/b \in \mathbb{Q} \mid a, b \in \mathbb{Z} \text{ and } p \nmid b\}$ be the localized ring by p and $\mathbb{F}_p[X]$ the polynomial ring over the finite field of order p. We denote by ϕ_p the canonical projection $\mathbb{Z}_{(p)}[X] \to \mathbb{F}_p[X]$. For $F \subset \mathbb{Q}[X]$, we denote by $I(F)$ the ideal generated by F. For $F \subset \mathbb{Z}_{(p)}[X]$, we denote $\langle \phi_p(F) \rangle$ by $I_p(F)$ and $\phi_p(I(F) \cap \mathbb{Z}_{(p)}[X])$ by $I_p^0(F)$.

We recall an outline of "modular algorithm for ideal operation" (see [24]) as Algorithm 3. Given ideals I, J, ideal operations $AL(*,*)$ over $\mathbb{Q}[X]$ and $AL_p(*,*)$ over $\mathbb{F}_p[X]$ as inputs, we compute $AL(I, J)$ as the output by using modular computations. First, we choose a list of random prime numbers $\mathcal{P}$, which satisfies certain computable condition PRIMETEST. For example, PRIMETEST is to check whether p is permissible (see Definition 5.2.1) for Gröbner bases of I and J or not. Next, we compute modular operations $H_p = AL_p(I, J)$ for each $p \in \mathcal{P}$. After omitting expected unlucky primes by DELETEUNLUCKYPRIMES, we lift H_p's up to H_{can} by CRT and rational reconstruction. Finally, we check if H_{can} is really the correct answer by FINALTEST. If FINALTEST says FALSE, then we enlarge $\mathcal{P}$ and continue from the first step. In this thesis, we introduce new FINALTEST for ideal quotient and DIQ. We remark that the termination of this modular algorithm is ensured by the finiteness of unlucky prime numbers. For example, for a given ideals I, J and an algorithm for the ideal quotient $(I : J)$ over the rational numbers, there are only finitely many steps from the inputs to the outputs and thus the number of coefficients is also finite; hence we can project the computations onto those over finite fields $\mathbb{F}_p$ for all prime numbers p except those dividing some denominators appearing in coefficients (see Lemma 6.1 in [24] for details).

Algorithm 3 Modular Algorithm for Ideal Operation

Input: I, J: ideals, $AL(*,*)$: an ideal operation over $\mathbb{Q}[X]$, $AL_p(*,*)$: an ideal operation over $\mathbb{F}_p[X]$

Output: $AL(I,J)$ over $\mathbb{Q}[X]$

```
choose P as a list of random primes satisfying primeTest
HP ← ∅
while do
  for p ∈ P do
    H_p ← AL_p(I, J)
    HP ← HP ∪ {H_p}
  end for
  (HP_lucky, P_lucky) ← deleteUnluckyPrimes(HP, P)
  lift HP_lucky to H_can by CRT and rational reconstruction
  if H_can passes finalTest then
    return H_can
  end if
  enlarge P with prime numbers not used so far
end while
```

First, we introduce some notions of *good* primes as follows.

Definition 5.2.1 ([24], Definition 2.1)**.** *Let p be a prime number, $F \subset \mathbb{Q}[X]$ and $\prec$ a monomial ordering. Let G be the reduced Gröbner basis of $I(F)$ with respect to $\prec$.*

(1) p is said to be weak permissible *for F, if $F \subset \mathbb{Z}_{(p)}[X]$.*

(2) p is said to be permissible *for F and $\prec$, if p is weak permissible for $F \subset \mathbb{Q}[X]$ and $\phi_p(\mathrm{lc}_\prec(f)) \neq 0$ for all f in F.*

(3) p is said to be compatible *with F if p is weak permissible for F and $I_p^0(F) = I_p(F)$.*

(4) p is said to be effectively lucky *for F and $\prec$, if p is permissible for $(G, \prec)$ and $\phi_p(G)$ is the reduced Gröbner basis of $I_p(G)$.*

Remark 5.2.2. *If p is effectively lucky for F and $\prec$, then p is compatible with F (see Lemma 3.1 (3) in [24]).*

Next, the notion of *p-compatible Gröbner basis candidate* is very useful for easily computable tests toward finalTest in modular techniques .

Definition 5.2.3 ([24], Definition 4.1)**.** *Let G_{can} be a finite subset of $\mathbb{Q}[X]$ and $F \subset \mathbb{Q}[X]$. We call G_{can}* a p-compatible Gröbner basis candidate *for F and $\prec$, if p is permissible for G_{can} and $\phi_p(G_{can})$ is a Gröbner basis of $I_p^0(F)$ with respect to $\prec$.*

The following can be used to finalTest in modular techniques.

Lemma 5.2.4 ([24], Proposition 4.1)**.** *Suppose that G_{can} is a p-compatible Gröbner basis candidate for $(F, \prec)$, and $G_{can} \subset I(F)$. Then G_{can} is a Gröbner basis of $I(F)$ with respect to $\prec$.*

We introduce the following easily computable tests for ideal quotient and saturation in modular techniques, appearing in [24].

Lemma 5.2.5 ([24], Lemma 6.2 and Lemma 6.4)**.** *Suppose that a prime number p is compatible with $(F, \prec)$ and permissible for $(f, \prec)$. For a finite subset $H_{can} \subset \mathbb{Q}[X]$, H_{can} is a Gröbner basis of $(I(F) : \langle f \rangle)$ with respect to $\prec$, if the following conditions hold;*

(1) p is permissible for $(H_{can}, \prec)$,

(2) $\phi_p(H_{can})$ is a Gröbner basis of $(I_p(F) : \langle \phi_p(f) \rangle)$ with respect to $\prec$,

(3) $H_{can} \subset (I(F) : \langle f \rangle)$.

For a finite subset $L_{can} \subset \mathbb{Q}[X]$, L_{can} is a Gröbner basis of $(I(F) : \langle f \rangle^\infty)$ with respect to $\prec$, if the following conditions hold;

(1) p is permissible for $(L_{can}, \prec)$,

(2) $\phi_p(L_{can})$ is a Gröbner basis of $(I_p(F) : \langle \phi_p(f) \rangle^\infty)$ with respect to $\prec$,

(3) $L_{can} \subset (I(F) : \langle f \rangle^\infty)$.

We generalize Lemma 5.2.5 by replacing f into an ideal J as follows. We recall that $I_p(G) = \langle \phi_p(G) \rangle_{\mathbb{F}_p[X]}$ where p is weak permissible for G.

Lemma 5.2.6 ([15], Lemma 2.2.6)**.** *Suppose that a prime number p is compatible with $(F, \prec)$ and permissible for $(G, \prec)$. For a finite subset $H_{can} \subset \mathbb{Q}[X]$, H_{can} is a Gröbner basis of $(I(F) : I(G))$ with respect to $\prec$, if the following conditions hold;*

(1) p is permissible for $(H_{can}, \prec)$,

(2) $\phi_p(H_{can})$ is a Gröbner basis of $(I_p(F) : I_p(G))$ with respect to $\prec$,

(3) $H_{can} \subset (I(F) : I(G))$.

Proof. Since p is permissible for $(H_{can}, \prec)$, we can consider $I_p(H_{can}) = \langle \phi_p(H_{can}) \rangle$. It is enough to show that $I_p(H_{can}) = \phi_p((I(F) : I(G)) \cap \mathbb{Z}_{(p)}[X])$ since the equation implies H_{can} is a p-compatible Gröbner basis candidate for $(I(F) : I(G))$ with respect to $\prec$ and a Gröbner basis of $(I(F) : I(G))$ with respect to $\prec$ from $H_{can} \subset (I(F) : I(G))$ and Lemma 5.2.4.

It is clear that $I_p(H_{can}) \subset \phi_p((I(F) : I(G)) \cap \mathbb{Z}_{(p)}[X])$ as $H_{can} \subset (I(F) : I(G))$. To show the inverse inclusion, we pick $h \in (I(F) : I(G)) \cap \mathbb{Z}_{(p)}[X]$. Then, $hG \subset I(F) \cap \mathbb{Z}_{(p)}[X]$ where $hG = \{hg \mid g \in G\}$ since p is permissible for h and G. Thus,

$$\begin{aligned} \phi_p(h) I_p(G) = \phi_p(h) \langle \phi_p(G) \rangle &= \langle \phi_p(hG) \rangle \\ &\subset \langle \phi_p(I(F) \cap \mathbb{Z}_{(p)}[X]) \rangle = I_p^0(F) = I_p(F) \end{aligned}$$

by the compatibility of F; we obtain that $\phi_p(h) \in (I_p(F) : I_p(G)) = I_p(H_{can})$. Hence $I_p(H_{can}) \supset \phi_p((I(F) : I(G)) \cap \mathbb{Z}_{(p)}[X])$. □

Remark 5.2.7. *We can check whether $H_{can} \subset (I(F) : I(G))$ or not, by checking whether $I(H_{can}) I(G) \subset I(F)$ or not.*

We apply this lemma to DIQ as follows.

Theorem 5.2.8 ([15], Theorem 2.2.8)**.** *Suppose that a prime number p is compatible with $(F, \prec)$ and permissible for $(G, \prec)$. Assume p satisfies $(I_p(F) : I_p(G)) = \phi_p((I(F) : I(G)) \cap \mathbb{Z}_{(p)}[X])$. For a finite subset $K_{can} \subset \mathbb{Q}[X]$, K_{can} is a Gröbner basis of $(I(F) : (I(F) : I(G)))$ with respect to $\prec$ if the following conditions hold;*

(1) p is permissible for $(K_{can}, \prec)$,

(2) $\phi_p(K_{can})$ is a Gröbner basis of $(I_p(F) : (I_p(F) : I_p(G)))$ with respect to $\prec$,

(3) $K_{can} \subset (I(F) : (I(F) : I(G)))$.

Proof. Since p is permissible for $(K_{can}, \prec)$, we can consider $I_p(K_{can}) = \langle \phi_p(K_{can}) \rangle$. By Lemma 5.2.4, it is enough to show that K_{can} is a p-compatible Gröbner basis candidate of $(I(F) : (I(F) : I(G)))$. Since $K_{can} \subset (I(F) : (I(F) : I(G)))$, $I_p(K_{can}) \subset \phi_p((I(F) : (I(F) : I(G))) \cap \mathbb{Z}_{(p)}[X])$ holds. Thus, we show the other inclusion. Let $h \in (I(F) : (I(F) : I(G))) \cap \mathbb{Z}_{(p)}[X]$. Then,

$$\phi_p(h)\phi_p((I(F) : I(G)) \cap \mathbb{Z}_{(p)}[X]) \subset \phi_p(I(F) \cap \mathbb{Z}_{(p)}[X]) = I_p^0(F) = I_p(F).$$

Since $\phi_p((I(F) : I(G)) \cap \mathbb{Z}_{(p)}[X]) = (I_p(F) : I_p(G))$, we obtain that $\phi_p(h) \in (I_p(F) : (I_p(F) : I_p(G))) = I_p(K_{can})$. Hence, $I_p(K_{can}) \supset \phi_p((I(F) : (I(F) : I(G))) \cap \mathbb{Z}_{(p)}[X])$. □

To check the conditions $(I_p(F) : I_p(G)) = \phi_p((I(F) : I(G)) \cap Z_{(p)}[X])$ and $K_{can} \subset (I(F) : (I(F) : I(G)))$, we need a Gröbner basis H of $(I(F) : I(G))$ in general (the former by $I_p(H) = (I_p(F) : I_p(G))$ and the latter by $I(K_{can})I(H) \subset I(F)$, respectively). However, as to the latter, in a special case that P is an associated prime divisor of I, we confirm it more easily. Setting $I(G) = P$ for a prime ideal P, we devise the following "Modular Associated Test" using modular techniques.

Theorem 5.2.9 (Modular Associated Test; [15], Theorem 2.2.9)**.** *Let I be an ideal and P a prime ideal. Let F and G be Gröbner bases of I and P respectively. Suppose p is permissible for F, G and satisfies $(I_p(F) : I_p(G)) = \phi_p((I(F) : I(G)) \cap \mathbb{Z}_{(p)}[X])$. Let K_{can} be a finite subset of $\mathbb{Q}[X]$. Then, P is a prime divisor of I if the following conditions hold;*

(1) p is permissible for $(K_{can}, \prec)$,

(2) $\phi_p(K_{can})$ is a Gröbner basis of $(I_p(F) : (I_p(F) : I_p(G)))$ with respect to $\prec$,

(3) $(I_p(F) : (I_p(F) : I_p(G))) = I_p(G)$,

(4) $K_{can} \subset P$.

Proof. To prove this, we use Theorem 5.2.8. If all conditions in Theorem 5.2.8 hold, then K_{can} is a Gröbner basis of $(I : (I : P))$ and thus $(I : (I : P)) \subset P$ by the condition $K_{can} \subset P$; hence, P is a prime divisor of I by Theorem 3.3.1. Now, we show that all conditions in Theorem 5.2.8 hold. Since we have directly (1) and (2) in Theorem 5.2.8, it is enough to check the condition $K_{can} \subset (I(F) : (I(F) : I(G)))$. Indeed, we obtain that $K_{can} \subset P \subset (I(F) : (I(F) : I(G)))$ by Remark 5.1.1 and (4). □

In the above associated test, K_{can} will coincide with G if P is a prime divisor of I. Thus, we can omit CRT and rational reconstruction as follows. Also, we minimize the number of prime numbers we use since we can check the number is large enough comparing with the following $\|G\|$. For a finite set G of $\mathbb{Q}[X]$, we define

$$\|G\| = \max\left\{a^2 + b^2 \mid \frac{a}{b} \text{ is a coefficient in a term of an element of } G\right\}.$$

Corollary 5.2.10 (Modular Associated Test without CRT, Algorithm 4; [15], Corollary 2.2.10)**.** *Let I be an ideal and P a prime ideal. Let F and G be Gröbner bases of I and P respectively. Let $\mathcal{P}$ be a finite set of prime numbers. Suppose every $p \in \mathcal{P}$ is permissible for F, G and satisfies $(I_p(F) : I_p(G)) = \phi_p((I(F) : I(G)) \cap \mathbb{Z}_{(p)}[X])$. Then, P is a prime divisor of I if the following conditions hold;*

(1) $(I_p(F) : (I_p(F) : I_p(G))) = I_p(G)$ for every $p \in \mathcal{P}$,

(2) $\prod_{p\in\mathcal{P}} p$ is larger than $\|G\|$.

Proof. Since $\prod_{p\in\mathcal{P}} p$ is larger than coefficients appearing in G for the rational reconstruction (see Lemma 4.2. in [7]), G is a Gröbner basis candidate itself and we can set $K_{can} = G$ in Theorem 5.2.9. Then, K_{can} satisfies all conditions in the theorem. □

Algorithm 4 Modular Associated Test without CRT

Input: F: a Gröbner basis of an ideal I, G: a Gröbner basis of a prime ideal P, H: a Gröbner basis of $(I(F) : I(G))$

Output: TRUE if P is a prime divisor of I

```
choose P as a list of random primes satisfying primeTest (p ∈ P is permissible for F, G and
H) and ∏_{p∈P} p > ‖G‖;
RESTART
while do
  for p ∈ P do
    if (I_p(F) : (I_p(F) : I_p(G))) ≠ I_p(G) then
      delete p from P
    end if
  end for
  if ∏_{p∈P} p ≤ ‖G‖ then
    enlarge P with prime numbers not used so far and go back to RESTART
  end if
  if (I_p(F) : I_p(G)) = I_p(H) for every p ∈ P then
    return TRUE
  end if
  enlarge P with prime numbers not used so far and go back to RESTART
end while
```

Also, we devise a non-associated test as follows. The test is useful since it does not need a condition $(I_p(F) : I_p(G)) = \phi_p((I(F) : I(G)) \cap \mathbb{Z}_{(p)}[X])$.

Algorithm 5 Modular Non-Associated Test

Input: F: a Gröbner basis of an ideal I, G: a Gröbner basis of a prime ideal P, H: a Gröbner basis of $(I(F) : I(G))$

Output: FALSE if P is NOT a prime divisor of I

```
choose 𝒫 as a list of random primes satisfying primeTest
𝒦𝒫 ← ∅
while do
  for p ∈ 𝒫 do
    K_p ← (I_p(F) : (I_p(F) : I_p(G)))
    if (I_p(F) : (I_p(F) : I_p(G))) = I_p(G) then
      delete p from 𝒫
    else
      𝒦𝒫 ← 𝒦𝒫 ∪ {K_p}
    end if
  end for
  (𝒦𝒫_lucky, 𝒫_lucky) ← deleteUnluckyPrimes(𝒦𝒫, 𝒫)
  lift 𝒦𝒫_lucky to K_can by CRT and rational reconstruction
  if I(K_can)I(H) ⊂ I then
    return False
  end if
  enlarge 𝒫 with prime numbers not used so far;
end while
```

Theorem 5.2.11 (Modular Non-Associated Test, Algorithm 5; [15], Theorem 2.2.11)**.** *Let I be an ideal and P a prime ideal. Let F and G be Gröbner bases of I and P respectively. Suppose p is permissible for F and G. Let $K_{can} \subset \mathbb{Q}[X]$ and we assume that p is permissible for K_{can}. Then, P is not a prime divisor of I if the following conditions hold;*

(1) $\phi_p(K_{can})$ is a Gröbner basis of $(I_p(F) : (I_p(F) : I_p(G)))$ with respect to $\prec$,

(2) $K_{can} \subset (I : (I : P))$,

(3) $(I_p(F) : (I_p(F) : I_p(G))) \neq I_p(G)$.

Proof. Suppose P is a prime divisor of I. Then, $(I : (I : P)) = P$ from Remark 5.1.1 and

$$\begin{aligned}\phi_p(K_{can}) &\subset \phi_p((I : (I : P)) \cap \mathbb{Z}_{(p)}[X]) \\ &= \phi_p(P \cap \mathbb{Z}_{(p)}[X]) = I_p^0(G) = I_p(G).\end{aligned}$$

Since $\langle \phi_p(K_{can}) \rangle = (I_p(F) : (I_p(F) : I_p(G))) \supset I_p(G)$, we obtain that $(I_p(F) : (I_p(F) : I_p(G)) = I_p(G)$. This contradicts $(I_p(F) : (I_p(F) : I_p(G))) \neq I_p(G)$. □

Next, we consider *modular saturation*. Since $(I : J^m) = (I : J^\infty)$ for a sufficiently large m, the following holds from Lemma 5.2.6.

Lemma 5.2.12 ([15], Lemma 2.2.12)**.** *Suppose that a prime number p is compatible with $(F, \prec)$ and permissible for $(G, \prec)$. For a finite subset $H_{can} \subset \mathbb{Q}[X]$, H_{can} is a Gröbner basis of $(I(F) : I(G)^\infty)$ with respect to $\prec$, if the following conditions hold;*

(1) p is permissible for $(H_{can}, \prec)$,

(2) $\phi_p(H_{can})$ is a Gröbner basis of $(I_p(F) : I_p(G)^\infty)$ with respect to $\prec$,

(3) $H_{can} \subset (I(F) : I(G)^\infty)$.

To check $H_{can} \subset (I(F) : I(G)^\infty)$, we can use the following.

Lemma 5.2.13 ([15], Lemma 2.2.13)**.** *Let H_{can}, F and G be finite subsets of $K[X]$. For $G = \{f_1, \ldots, f_k\}$ and a positive integer m, we denote $\{f_1^m, \ldots, f_k^m\}$ by $G^{[m]}$. Then, the following conditions are equivalent.*
(A) $H_{can} \subset (I(F) : I(G)^\infty)$,
(B) $I(H_{can})I(G)^m \subset I(F)$ for some m,
(C) $I(H_{can})I(G^{[m]}) \subset I(F)$ for some m.

Proof. First, we show that (A) implies (B). This is obvious from the definition of $(I(F) : I(G)^\infty)$. Next, we show that (B) implies (C). Since $I(G^{[m]}) \subset I(G)^m$, $I(H_{can})I(G^{[m]}) \subset I(H_{can})I(G)^m \subset I(F)$. Finally, we show that (C) implies (A). As $I(G)^{km} \subset I(G^{[m]})$, we obtain that $I(H_{can})I(G)^{km} \subset I(H_{can})I(G^{[m]}) \subset I(F)$ and $H_{can} \subset (I(F) : I(G)^\infty)$. □

Since the number of generators of $I(G^{[m]})$ is less than that of $I(G)^m$, it is better to check whether $I(H_{can})I(G^{[m]}) \subset I(F)$ or not.

Finally, we introduce modular techniques for *double saturation (the second saturated quotient).*

Theorem 5.2.14 ([15], Theorem 2.2.14)**.** *Suppose that a prime number p is compatible with $(F, \prec)$ and permissible for $(G, \prec)$. Assume p satisfies $(I_p(F) : I_p(G)^\infty) = \phi_p((I(F) : I(G)^\infty) \cap \mathbb{Z}_{(p)}[X])$. For a finite subset $K_{can} \subset \mathbb{Q}[X]$, K_{can} is a Gröbner basis of $(I(F) : (I(F) : I(G)^\infty)^\infty)$ with respect to $\prec$ if the following conditions hold;*

(1) p is permissible for $(K_{can}, \prec)$,

(2) $\phi_p(K_{can})$ is a Gröbner basis of $(I_p(F) : (I_p(F) : I_p(G)^\infty)^\infty)$ with respect to $\prec$,

(3) $K_{can} \subset (I(F) : (I(F) : I(G)^\infty)^\infty)$.

Proof. For a sufficiently large integer m, $(I(F) : I(G)^\infty) = (I(F) : I(G)^m)$ and $(I_p(F) : I_p(G)^\infty) = (I_p(F) : I_p(G)^m)$. Thus, we can prove this by the similar way of Theorem 5.2.8. □

5.3 Intermediate Primary Decomposition

In this section, we introduce *intermediate primary decomposition* as a bi-product of modular localizations devised in Section 5.2. We give a rough outline of possible "intermediate primary decomposition via MIS". The idea of modular primary decomposition comes from [29]. In general, modular primary decomposition is very difficult to compute since primary component may be different over infinite many finite fields. For example, $I = \langle x^2 + 1 \rangle \cap \langle x + 1 \rangle$ is a primary decomposition in $\mathbb{Q}[X]$, however, it is not one in $\mathbb{F}_p[X]$ for every prime number p of type $p = 4n + 1$. Thus, we propose *intermediate primary decomposition via MIS* instead of full primary decomposition. Then, for a subset $U \subset X$, we define

$$\mathrm{Ass}_U(I_p(F)) = \{\bar{P}_p \in \mathrm{Ass}(I_p(F)) \mid U \text{ is an MIS of } \bar{P}_p\}.$$

where p is permissible for F. Also, we denote the set of prime divisors of I which have the same MIS U by

$$\mathrm{Ass}_U(I) = \{P \in \mathrm{Ass}(I) \mid U \textit{ is an MIS of } P\}.$$

We note that U is an MIS of $I(F)$ if U is one of the initial ideal $\langle \mathrm{lt}_\prec(I(F))\rangle$ (see Exercise 3.5.1 in [13]). Thus, if p is effective lucky for $(F,\prec)$ and U is an MIS of $\langle \mathrm{lt}_\prec(I(F))\rangle$ then U is also an MIS of $I(F)$ and $I_p(F)$. Here, we define intermediate primary decomposition in general setting as follows (a certain generalization of one in [26]).

Definition 5.3.1 ([15], Definition 2.3.1)**.** *Let I be an ideal. Then, a set of ideals $\mathcal{Q}$ is called an* intermediate primary decomposition (IPD) *of I if*

(a) for all $Q \in \mathcal{Q}$, $\mathrm{Ass}(Q) \subset \mathrm{Ass}(I)$,

(b) $\bigcap_{Q\in\mathcal{Q}} Q = I$.

We call $Q \in \mathcal{Q}$ an intermediate primary component of I. In particular, when there is a subset U of X s.t. $\mathrm{Ass}(Q) = \mathrm{Ass}_U(I)$*, we call Q an intermediate component of I via U.*

We remark that $\bigcup_{Q\in\mathcal{Q}} \mathrm{Ass}(Q) = \mathrm{Ass}(I)$. For computing intermediate primary decomposition, the following corollary is very useful to generate prime divisors.

Corollary 5.3.2 ([15], Corollary 2.3.2)**.** *Let F be a Gröbner basis of I and p a permissible prime number for F. Let U be a subset of X such that* $\mathrm{Ass}_U(I_p(F))$ *is not empty, and $\bar{H}$ a Gröbner basis of $\bar{J} = \bigcap_{P_p\in\mathrm{Ass}_U(I_p(F))} P_p$. Let H_{can} be a Gröbner basis candidate constructed from $\bar{H}$ and $J = I(H_{can})$. Assume p is permissible for H_{can}. Suppose H_{can} is a Gröbner basis of J and p is effectively lucky for the reduced Gröbner basis L of $(I : J)$ with $I_p(L) = (I_p(F) : I_p(H_{can}))$. If J is a prime ideal then J is a prime divisor of I.*

Proof. To apply Theorem 5.2.9 for I and J, we check the conditions. First, since p is effectively lucky for L, p is compatible with L by Remark 5.2.2. Thus, $\phi_p((I(F) : I(H_{can}))\cap\mathbb{Z}_{(p)}[X]) = I_p^0(L) = I_p(L) = (I_p(F) : I_p(H_{can}))$. From the assumption, p is permissible for H_{can}. As $I_p(H_{can}) = \bar{J}$ is an intersection of equidimensional prime divisors of $I_p(F)$, it follows that $(I_p(F) : (I_p(F) : I_p(H_{can})) = I_p(H_{can})$ by Theorem 5.1.3. Thus, $\phi_p(H_{can}) = \bar{H}$ is a Gröbner basis of $(I_p(F) : (I_p(F) : I_p(H_{can}))$. It is obvious that $H_{can} \subset J$. Hence, all conditions in Theorem 5.2.9 hold and thus J is a prime divisor of I. □

When J is not prime, we can check the radicality of J by the following lemma. For any effectively lucky p for H_{can}, if $\langle\bar{H}\rangle$ is radical then $\langle H_{can}\rangle$ is also radical.

Lemma 5.3.3 ([24], Lemma 6.7)**.** *Suppose that H_{can} is the output of our CRT modular computation, that is, it satisfies the following:*

(1) p is permissible for $(H_{can}, \prec)$,

(2) $\phi_p(H_{can})$ coincides with the reduced Gröbner basis of $\sqrt{I_p(F)}$

(3) $H_{can} \subset \sqrt{I(F)}$

Then H_{can} is the reduced Gröbner basis of $\sqrt{I(F)}$ with respect to $\prec$.

We can extend Corollary 5.3.2 to an intersection of prime divisors by using Theorem 5.1.3 as Proposition 5.3.4. We can ensure that the lifted ideal $I(H_{can})$ is radical from Lemma 5.3.3 and an intersection of prime divisors I from Theorem 5.1.3 and Theorem 5.2.8.

Proposition 5.3.4 ([15], Proposition 2.3.4)**.** *Under the conditions of Corollary 5.3.2 (except the primality of J), if J is a radical ideal then J is some intersections of prime divisors of I.*

We note that, if $\mathrm{Ass}_U(I_p(F))$ consists of one prime, that is, $\bar{J}$ is prime, then we check if J is prime or not more easily. Moreover, if $\mathrm{Ass}_U(I_p(F))$ consists of two prime ideals $\bar{P}_1$ and $\bar{P}_2$ and then we combine those prime divisors and apply the criterion for radical to the lifting of $\bar{P}_1 \cap \bar{P}_2$. We also make the same argument for $\bar{P}_1 \cap \bar{P}_2 \cap \bar{P}_3$, $\bar{P}_1 \cap \bar{P}_2 \cap \bar{P}_3 \cap \bar{P}_4$ and so on.

Example 5.3.5. *Let $I = \langle x\rangle \cap \langle x^3, y\rangle \cap \langle x^2+1\rangle \subset \mathbb{Q}[x, y]$. Let $F = \{x^3y+xy, x^5+x^3\}$ be the reduced Gröbner basis of I. We consider two prime numbers $p = 3, 5$. Then, $\mathrm{Ass}(I_3(F)) = \{\langle x\rangle, \langle x, y\rangle, \langle x^2+1\rangle\}$ and $\mathrm{Ass}(I_5(F)) = \{\langle x\rangle, \langle x, y\rangle, \langle x+2\rangle, \langle x+3\rangle\}$. For $U_1 = \{y\}$ and $U_2 = \emptyset$, $\mathrm{Ass}_{U_1}(I_3(F)) = \{\langle x\rangle, \langle x^2+1\rangle\}$ and $\mathrm{Ass}_{U_2}(I_3(F)) = \{\langle x, y\rangle\}$. Similarly, $\mathrm{Ass}_{U_1}(I_5(F)) = \{\langle x\rangle, \langle x+2\rangle, \langle x+3\rangle\}$ and $\mathrm{Ass}_{U_2}(I_5(F)) = \{\langle x, y\rangle\}$. For $J_p(U) = \bigcap_{P_p \in \mathrm{Ass}_U(I_p(F))} P_p$, it follows that $J_3(U_1) = \langle x^3+x\rangle$, $J_5(U_1) = \langle x^3+x\rangle$, $J_3(U_2) = \langle x, y\rangle$ and $J_5(U_2) = \langle x, y\rangle$. By using CRT, we may compute radicals of intermediate primary components $J_{can}(U_1) = \langle x^3+x\rangle$ and $J_{can}(U_2) = \langle x, y\rangle$. Finally, we obtain an intermediate primary decomposition $\{\langle x^3+x\rangle, \langle x^3, y\rangle\}$ of I from Lemma 5.1.5 and Theorem 5.1.7.*

Finally, we sketch an outline of intermediate primary decomposition via MIS as follows. Its termination comes from the finiteness of unlucky primes for computation of associated prime divisors and primary components.

Intermediate Primary Decomposition via MIS

Input: F: a Gröbner basis of an ideal I.

Output: $\{Q(U)\}$: an IPD via MIS of I.

(Step 1) choose $\mathcal{P}$ as a list of random primes satisfying PRIMETEST

(Step 2) compute $\mathrm{Ass}(I_p(F))$ for $p \in \mathcal{P}$ and choose a set of MISs $\mathcal{U}$ from $\mathrm{Ass}(I_p(F))$

(Step 3) compute $J_p(U) = \bigcap_{P_p \in \mathrm{Ass}_U(I_p(F))} P_p$ for each $U \in \mathcal{U}$ and let $\mathcal{JP}(U) = \mathcal{JP}(U) \cup \{J_p(U)\}$

(Step 4) delete unlucky p for $\mathcal{JP}(U)$ and obtain $\mathcal{JP}_{lucky}(U)$

(Step 5) lift $\mathcal{JP}_{lucky}(U)$ to $J_{can}(U)$ by CRT and rational reconstruction. If $J_{can}(U)$ is unmixed then go to Step 6; otherwise RESTART

(Step 6) if $J_{can}(U)$ passes FINALTEST (Proposition 5.3.4) then go to Step 7: otherwise RESTART

(Step 7) compute an intersection of primary components $Q(U)$ by $\mathrm{hull}(I + J_{can}(U)^m)$ (Lemma 5.1.5 and 5.1.6) or $\mathrm{hull}((I : (I : J_{can}(U)^\infty)^\infty))$ (Theorem 5.1.7) for isolated cases

(Step 8) if $\bigcap_{U \in \mathcal{U}} Q(U) = I$ then return $\{Q(U)\}$; otherwise RESTART

RESTART: enlarge $\mathcal{P}$ with prime numbers not used so far and go back to Step 2

Chapter 6

Experiments

In this chapter, we see computational experiments on our algorithms. Since it is very difficult to analyze the complexity of Gröbner basis computation, we compare the timings of implemented algorithms instead. From the experiments, we see that LPAs have clearly effectiveness by their specialities and each LPA has its characteristics coming from its effective techniques. Also, we examined the efficiency of modular techniques for ideal quotients by computational experiments.

6.1 Experiments on LPAs

We made an implementation on the computer algebra system Risa/Asir [25] and apply it to several examples as experiments. We revisited old examples in [17], $I_1(n)$ and $A_{k,m,n}$. The former $I_1(n) = \langle x^2 \rangle \cap \langle x^4, y \rangle \cap \langle x^3, y^3, (z+1)^n + 1 \rangle$ is an ideal whose embedded primary components are not easy to compute. If n is considerable large, it is difficult to compute a full primary decomposition of $I_1(n)$ though the isolated divisor $P_1 = \langle x \rangle$ can be detected pretty easily. The latter $A_{k,m,n}$ defined in [27] is more valuable for mathematics and its primary decomposition has important meanings in Computer Algebra for Statistics. We newly considered $T_1, \ldots, T_{10}$ that appear in [19] for benchmarks of effective localization. We describe the more details of ideals in Section 6.1.4. Timings are measured on a PC with Intel Core i7-8700B CPU with 32GB memory.

Now, we explain the details of Local Primary Algorithms (LPAs). From Proposition 1.4.6, the primitive LPA (LPA-0) use *double ideal quotient* and *regular sequence* to compute *equidimensional hull*. To compute a regular sequence in $I + P_G^{[m]}$ and one in $(I : (I : P^\infty)^\infty)$ efficiently, we use Lemma 4.2.5 and Corollary 4.2.6 respectively. As improved versions, LPA-$P_G^{[m]}$ is an implementation based on Lemma 4.2.3 and LPA-MIS is one from Lemma 4.2.7 and Criteria 3, 4. Both methods are implemented in LPA-($P_G^{[m]}$+MIS). The new algorithm LPA-($P_G^{[m]}$+MIS) without DIQ is based on Algorithm 2. In all figures, the horizontal axis shows isolated or embedded prime divisors and the vertical axis represents the timing (in seconds) of each prime divisor. In particular, the embedded prime divisors are in decreasing order of their dimensions.

6.1.1 Computation of Isolated Components

First, we apply LPAs to isolated primary components. In Table 6.1, for many cases, we can see that LPAs have clearly effectiveness by their specialities. We call an algorithm *stable* for an ideal if the *statistical standard deviation* of timing data for their prime divisors is small. Figure 6.1 and Table

6.2 show that LPA-0 is stable for T_1 since the the statistical standard deviation is 4.17, which is much smaller than those of LPA-MIS and LPA-($P_G^{[m]}$+MIS). On the other hand, both LPA-MIS and LPA-($P_G^{[m]}$+MIS) without DIQ take much time for some cases and are unstable since the statistical standard deviations are over 100 times of that of LPA-0. Also, we can see its instability in Figures 6.2 and 6.3, where we limit the maximum to 35 seconds. The main reason is that MIS-localization becomes very time-consuming for specific ideals and prime ideals. However, when MIS-localization is efficient, timings of LPA-MIS and LPA-($P_G^{[m]}$+MIS) without DIQ are much faster than those of LPA-0. There are almost no difference between timings of LPA-MIS and LPA-($P_G^{[m]}$+MIS) without DIQ since MIS-localization is very effective and it can reduce the timings of other parts. As a summary of our analysis for isolated examples,

- LPAs have clearly effectiveness by their specialities.
- LPA-0 is stable, on the other hand, both LPA-MIS and LPA-($P_G^{[m]}$+MIS) without DIQ are unstable due to such *strange* behavior of MIS-localization. However, it is much useful than LPA-0 when MIS-localization works well.

Ideals\Algorithms	LPA-0	LPA-MIS	LPA-($P_G^{[m]}$+MIS) w/o DIQ
$I_1(100), P_1$	0.01	0.007	0.006
$I_1(200), P_1$	0.02	0.01	0.01
$I_1(300), P_1$	0.03	0.01	0.01
$I_1(400), P_1$	0.04	0.02	0.01
$I_1(500), P_1$	0.05	0.02	0.02
$A_{3,4,5}, P_2$	14.1	> 7200	> 7200
T_1, P_3	12.3	> 7200	> 7200
T_1, P_4	28.2	0.20	0.19
T_2, P_5	50.0	> 7200	> 7200
T_3, P_6	0.96	0.04	0.04
T_4, P_7	4.11	7.74	7.84
T_5, P_8	5.22	0.07	0.07
T_6, P_9	0.13	0.02	0.01
T_7, P_{10}	25.5	0.21	0.21
T_8, P_{11}	0.06	0.02	0.02
T_9, P_{12}	2.42	1.78	1.73
T_{10}, P_{13}	151	2.81	2.81

Table 6.1: Local Primary Algorithm (Isolated)

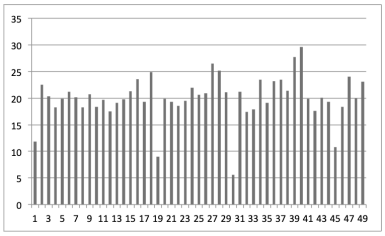

Figure 6.1: LPA-0 (49 isolated prime divisors of T_1)

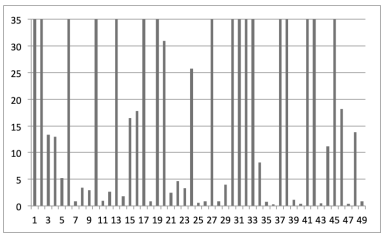

Figure 6.2: LPA-MIS (49 isolated prime divisors of T_1)

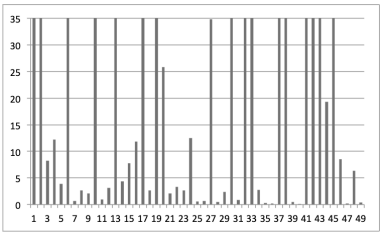

Figure 6.3: LPA-($P_G^{[m]}$+MIS) without DIQ (49 isolated prime divisors of T_1)

Ideals \ Algorithms	LPA-0	LPA-MIS (LPA-MIS/LPA-0)	LPA-($P_G^{[m]}$+MIS) w/o DIQ ((LPA-($P_G^{[m]}$+MIS) w/o DIQ)/LPA-0)
T_1	4.17	457 (109)	478 (114)
T_3	173	428 (2.47)	428 (2.47)
T_4	0.68	14.9(21.9)	14.8 (21.7)
T_5	2.65	541(204)	541 (204)
T_7	4.26	282(66.1)	281 (65.9)
T_8	327	438(1.33)	439 (1.34)
T_9	0.11	582 (5290)	584 (5309)
T_{10}	16.8	557 (33.1)	562 (33.4)

Table 6.2: The statistical standard deviations of timing data for isolated prime divisors, where we limit the maximum to 1200 seconds

6.1.2 Computation of Embedded Components

In Table 6.3, the primitive LPA (LPA-0) is not practical for some examples since the cost of computing hull($I + P^m$) is much high. Comparing LPA-0 and LPA-$P_G^{[m]}$ (also LPA-MIS and LPA-($P_G^{[m]}$+MIS)), we can see that the technique $P_G^{[m]}$-products is effective for most cases. As algorithms using MIS-localization, LPA-($P_G^{[m]}$+MIS) and LPA-($P_G^{[m]}$+MIS) without DIQ have good effectiveness by their specialities for many cases, for examples, $(I_1(n), P_{14})$, $(A_{2,4,4}, P_{15})$, $(A_{2,3,7}, P_{16})$, (T_1, P_{17}), (T_4, P_{21}), (T_7, P_{24}), (T_8, P_{25}), (T_{10}, P_{27}) and so on. From Table 6.3, we can see that MIS-technique is efficient for many cases. However, there are some examples s.t. MIS-localization

is not efficient, for instance, (T_1, P_{18}) and (T_3, P_{20}). In Figures 6.4, 6.5 and 6.7, we can see that LPAs using MIS are unstable due to MIS-localization, comparing them with LPA-$P_G^{[m]}$. Same as isolated components, there are almost no difference between timings of LPA-($P_G^{[m]}$+MIS) and those of LPA-($P_G^{[m]}$+MIS) without DIQ since MIS-localization is much powerful and we can ignore the timings for computation of DIQ. In summary,

- The technique $P_G^{[m]}$-products is effective for most cases.
- Both LPA-($P_G^{[m]}$+MIS) and LPA-($P_G^{[m]}$+MIS) without DIQ are much efficient to compute specific embedded components for most prime divisors.
- MIS-localization is very powerful but unstable, compared to LPA-$P_G^{[m]}$.

Ideals \ Algorithms	LPA-0	LPA-$P_G^{[m]}$	LPA-MIS	LPA-($P_G^{[m]}$+MIS)	LPA-($P_G^{[m]}$+MIS) w/o DIQ
$I_1(100), P_{14}$	0.09	0.07	0.01	0.01	0.007
$I_1(200), P_{14}$	0.17	0.14	0.02	0.02	0.01
$I_1(300), P_{14}$	0.29	0.25	0.02	0.02	0.01
$I_1(400), P_{14}$	0.41	0.31	0.03	0.03	0.02
$I_1(500), P_{14}$	0.43	0.38	0.03	0.02	0.03
$A_{2,4,4}, P_{15}$	1707	5.50	0.56	0.25	0.32
$A_{2,3,7}, P_{16}$	143	25.1	0.60	0.37	0.41
T_1, P_{17}	73.8	71.8	0.27	0.22	0.20
T_1, P_{18}	61.6	58.2	>7200	>7200	>7200
T_2, P_{19}	214	188	>7200	>7200	>7200
T_3, P_{20}	0.75	0.76	29.6	29.5	29.5
T_4, P_{21}	10.9	9.53	0.12	0.10	0.08
T_5, P_{22}	>7200	63.0	>7200	2.82	1.13
T_6, P_{23}	>7200	5.83	>7200	0.13	0.05
T_7, P_{24}	86.3	41.5	5.89	0.21	0.19
T_8, P_{25}	3.32	0.27	0.08	0.04	0.02
T_9, P_{26}	9.54	8.18	>7200	>7200	>7200
T_{10}, P_{27}	4338	256	668	0.89	0.80

Table 6.3: Local Primary Algorithm (Embedded)

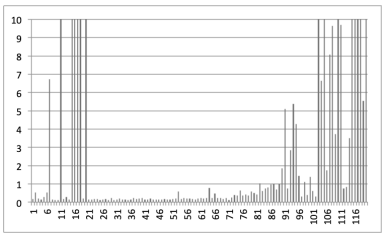

Figure 6.4: LPA-($P_G^{[m]}$+MIS)
(120 embedded prime divisors of T_1)
upper limit: 10 seconds

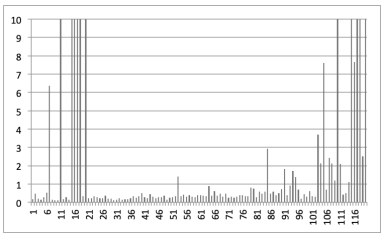

Figure 6.5: LPA-($P_G^{[m]}$+MIS) w/o DIQ
(120 embedded prime divisors of T_1)
upper limit: 10 seconds

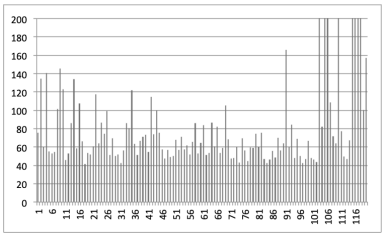

Figure 6.6: LPA-$P_G^{[m]}$
(120 embedded prime divisors of T_1)
upper limit: 200 seconds

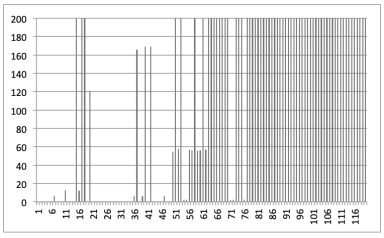

Figure 6.7: LPA-MIS
(120 embedded prime divisors of T_1)
upper limit: 200 seconds

6.1.3 Summary on Computational behavior

In isolated cases, LPAs have clearly effectiveness by their specialities. In embedded cases, the technique P_G^m-products is a useful way. For both cases, MIS-localization is very efficient for many ideals and prime divisors, however, it is unstable. To make our LPAs more effective and efficient, we need to improve DIQ or MIS-localization. Since methods without MIS (LPA-0 and LPA-$P_G^{[m]}$ are stable, those with improved DIQ will give us efficient and stable LPAs. On the other hand, if we succeed in improving the efficiency of MIS-localization, we will also have more efficient algorithms.

6.1.4 Ideals and Prime Ideals in Experiments

$$
\begin{aligned}
I_1(n) =& \langle x^2\rangle \cap \langle x^4, y\rangle \cap \langle x^3, y^3, (z+1)^n + 1\rangle \subset \mathbb{Q}[x, y, z].\\
A_{3,4,5} =& \langle (x_{12}x_{23} - x_{13}x_{22})x_{31} - x_{11}x_{32}x_{23} + x_{11}x_{33}x_{22} + (x_{13}x_{32} - x_{12}x_{33})x_{21},\\
& x_{13}x_{32} - x_{12}x_{33})x_{24} + (-x_{14}x_{32} + x_{12}x_{34})x_{23} + (x_{14}x_{33} - x_{13}x_{34})x_{22},\\
& (x_{14}x_{33} - x_{13}x_{34})x_{25} + (-x_{15}x_{33} + x_{35}x_{13})x_{24} + (x_{15}x_{34} - x_{35}x_{14})x_{23},\\
& (x_{42}x_{23} - x_{43}x_{22})x_{31} - x_{41}x_{32}x_{23} + x_{41}x_{33}x_{22} + (x_{43}x_{32} - x_{42}x_{33})x_{21},\\
& (x_{43}x_{32} - x_{42}x_{33})x_{24} + (-x_{44}x_{32} + x_{42}x_{34})x_{23} + (x_{44}x_{33} - x_{43}x_{34})x_{22},\\
& (x_{44}x_{33} - x_{43}x_{34})x_{25} + (-x_{45}x_{33} + x_{35}x_{43})x_{24} + (x_{45}x_{34} - x_{35}x_{44})x_{23}\rangle\\
& \subset \mathbb{Q}[x_{ij} \mid 1 \le i \le 4, 1 \le j \le 5].\\
A_{2,4,4} =& \langle -x_{21}x_{12} + x_{22}x_{11}, -x_{22}x_{13} + x_{23}x_{12}, -x_{23}x_{14} + x_{24}x_{13}, x_{32}x_{21} - x_{31}x_{22},\\
& x_{33}x_{22} - x_{32}x_{23}, x_{34}x_{23} - x_{24}x_{33}, x_{42}x_{31} - x_{41}x_{32}, x_{43}x_{32} - x_{42}x_{33},\\
& x_{44}x_{33} - x_{43}x_{34}\rangle \subset \mathbb{Q}[x_{ij} \mid 1 \le i \le 4, 1 \le j \le 4].
\end{aligned}
$$

$$
\begin{aligned}
A_{2,3,7} =&\langle -x_{21}x_{12}+x_{22}x_{11}, -x_{22}x_{13}+x_{23}x_{12}, -x_{23}x_{14}+x_{24}x_{13}, -x_{24}x_{15}+x_{25}x_{14},\\
&-x_{25}x_{16}+x_{26}x_{15}, -x_{26}x_{17}+x_{27}x_{16}, x_{32}x_{21}-x_{31}x_{22}, x_{33}x_{22}-x_{32}x_{23},\\
&x_{34}x_{23}-x_{24}x_{33}, x_{35}x_{24}-x_{25}x_{34}, x_{36}x_{25}-x_{26}x_{35}, x_{37}x_{26}-x_{36}x_{27}\rangle\\
&\subset \mathbb{Q}[x_{ij} \mid 1\le i\le 3, 1\le j\le 7].\\
T_1 =&\langle cdefghiz+cdefhjz+bcdeijz, 3cdfghz^3+4bdefghj+4bdehjz^2,\\
&2bfghijz+fhjz^3, 4bcefhz+cfgijz, cdjz, 3egjz^4+bcdgij+2cdhjz^2,\\
&3defiz+2defz^2+4bcei, 4bcefiz+3dfhjz^2, cefhjz+bcfiz^2+giz^4,\\
&4ceghiz+bcejz\rangle \subset \mathbb{Q}[b,c,d,e,f,g,h,i,j,z].\\
T_2 =&\langle 3bcegz^2+4bcghi+2bcez^2, bcez+3dhi, cfgiz^3+bcdegh, cfgz^4+\\
&3cdefgh, 2bcfgiz^2+bcdegh+z^6, bchz+4bcg, 4bcdgiz+2cfhiz^2+\\
&3bdfhi, bdefhz+bz^4, 3befgiz+2cefgz^2+4cfhz^2, 3bfh+4fhi+bz^2\rangle\\
&\subset \mathbb{Q}[b,c,d,e,f,g,h,i,z].\\
T_3 =&\langle 4befjkmz^3+2bcdhijlm+cdegkmz^2, cdeghjlz, 2defghilz+4jlz^6+\\
&defjlz^2, beghjlmz+4ceghiz^2+bdeflz^2\rangle \subset \mathbb{Q}[b,c,d,e,f,g,h,i,j,k,l,m,z].\\
T_4 =&\langle 2cfhiz^2+bdefh, bcfijz+4bcghi, 2cdejz+4cdfj+ijz^2, bcdfgijz+\\
&cdijz^3, 3bceijz+3cgijz^2+beiz^3, 4bchjz+cgiz^2, behj, 3cdefhiz+\\
&2bdfgjz+2bchjz^2\rangle \subset \mathbb{Q}[b,c,d,e,f,g,h,i,j,z].\\
T_5 =&\langle 4bc^2d^2e^2gh^2iz^2+b^2ciz^9+2bceg^2hz^5, bcd^2e^2g^2h^2, bcfhz^5+b^2dfg^2iz,\\
&4bc^2e^2f^2h^2i^2z^2+b^2c^2e^2fh^2iz^3, 2b^2de^2f^2hi^2z+3b^2c^2e^2h^2i^2\rangle\\
&\subset \mathbb{Q}[b,c,d,e,f,g,h,i,z].\\
T_6 =&\langle 4bcdfghlz+3bcfhlz^3, befhkl+defghz, 3bdefhijklz+2cfhjkz^5+\\
&bdehkz^4, 4befijkl+dgklz^3, bcdefghj+2bcdegijz+2bcdhjklz,\\
&cdegijz+3bcdefk+4fhklz^2, 2bdeghjkz+cdez^5+3eghjz^3,\\
&bcdghijz+cdfhklz+2bcdhkz^2, 2bcdefi+bhijkl, eghjkz^5+\\
&2bcefghjkl, gilz^2+2beil, g, 3cdefijkl+4bcdgjz^3, cdehijz+4cegjz^3,\\
&bchkl, cdfghklz+befhilz+cdfgjlz, fiz^5+2cdfghk+bdfhiz,\\
&befijklz^2+3bcdghijl, 2bgijklz+2bcghil+cefhjz, 2defghjz+\\
&3cefhijz+3bdghiz\rangle \subset \mathbb{Q}[b,c,d,e,f,g,h,i,j,k,l,z].\\
T_7 =&\langle cfghijklz+cdz^7, 3bdikz^7+3bcdefghikl+4bfghkz^5, 3befghijkz+\\
&2bcegijz^3, 3cfhjlz+dfhjlz+4bdfkl, 3bejz^4+bdfgjk+2begjz^2,\\
&cdefgjkz+3efgjlz^2+4elz^5, bcdefghjk, 4cehjlz^4+3ceghijkl,\\
&efghjklz, ik, 4beghijkz^3+3bdeghijkl, cdefkl+dgjklz, 2bghijlz+\\
&bcdgiz+4eghjkz, bcehijklz+cdghijlz^2, 2bcdefglz+2cfgijlz^2+\\
&chz^6, 4bdefhjlz+bdhijlz+2defgklz, 2cdgiklz+cehklz^2+4cghilz,\\
&chjkl, 2bcdhijlz+cgijz^4, bdfhijkz+4bdijkz^3+2dhlz^4\rangle\\
&\subset \mathbb{Q}[b,c,d,e,f,g,h,i,j,k,l,z].\\
T_8 =&\langle 3bejz^4+bdfgjk+2begjz^2, cdefgjkz+3efgjlz^2+4elz^5, bcdefghjk,\\
&4cehjlz^4+3ceghijkl\rangle \subset \mathbb{Q}[b,c,d,e,f,g,h,i,j,k,l,z]\\
T_9 =&\langle 3hz^4+2cdfg, bdefgh+cfgz^3+cgz^4, bcgz^2+cdef+defz, , 3efgh+
\end{aligned}
$$

$$
\begin{aligned}
&bcez + 2bfz^2, 3defh + 2cegh, dehz + 4cgz^2, 2cdefhz + chz^3, 3cdefhz + \\
&2cfghz, 3dfghz + 2efhz^2 + 2bcgz, bdhz + 2efz + 2bhz\rangle \\
&\subset \mathbb{Q}[b, c, d, e, f, g, h, z].
\end{aligned}
$$

$$
\begin{aligned}
T_{10} =&\langle 4cdfhjkz + 4efhijz^2 + cehiz^2, bcdfiz, 3bdefhj + 4cdeghz, cdegkz + \\
&bdiz^3, bcdkz^2 + 2begjk, 2cdefhijz + 3cehijz^3 + bcdhz^4, efhjkz + 3bcfhz, \\
&2bcegiz + 3dghijz + 3fghiz, bdfjz + dfjkz, 4efhikz + 3befhi + 2dfghi, \\
&cdhijz + 2efgkz^2, bcdgikz^2 + bcdfgik, dfgikz, 2bcdghiz + bcegiz^2 + \\
&bdfijk, cdefghijz, bcdegijkz + cdefkz^4, 4bdfghjz + bdgkz^3 + 2bcdeij, \\
&cefghijkz + 4defgikz^3 + 4eghkz^4, bcdgijkz + ceghjkz^2 + 4cefghz^3\rangle \\
&\subset \mathbb{Q}[b, c, d, e, f, g, h, i, j, k, z].
\end{aligned}
$$

$$
\begin{aligned}
P_1 =&\langle x\rangle \subset \mathbb{Q}[x, y, z].\\
P_2 =&\langle x_{13}, x_{23}, x_{33}, x_{43}\rangle \subset \mathbb{Q}[x_{ij} \mid 1 \le i \le 4, 1 \le j \le 5].\\
P_3 =&\langle b, z\rangle \subset \mathbb{Q}[b, c, d, e, f, g, h, i, j, z].\\
P_4 =&\langle e, i, z\rangle \subset \mathbb{Q}[b, c, d, e, f, g, h, i, j, z].\\
P_5 =&\langle g, h, z\rangle \subset \mathbb{Q}[b, c, d, e, f, g, h, i, z].\\
P_6 =&\langle h, z\rangle \subset \mathbb{Q}[b, c, d, e, f, g, h, i, j, k, l, m, z].\\
P_7 =&\langle b, j, z\rangle \subset \mathbb{Q}[b, c, d, e, f, g, h, i, j, z].\\
P_8 =&\langle f, g, i\rangle \subset \mathbb{Q}[b, c, d, e, f, g, h, i, z].\\
P_9 =&\langle z^4 + hdb, c, g, k, l\rangle \subset \mathbb{Q}[b, c, d, e, f, g, h, i, j, k, l, z].\\
P_{10} =&\langle b, c, e, h, i, j\rangle \subset \mathbb{Q}[b, c, d, e, f, g, h, i, j, k, l, z].\\
P_{11} =&\langle e, k\rangle \subset \mathbb{Q}[b, c, d, e, f, g, h, i, j, k, l, z].\\
P_{12} =&\langle e, g, z\rangle \subset \mathbb{Q}[b, c, d, e, f, g, h, z].\\
P_{13} =&\langle e, g, k, z\rangle \subset \mathbb{Q}[b, c, d, e, f, g, h, i, j, k, z].\\
P_{14} =&\langle x, y\rangle \subset \mathbb{Q}[x, y, z].
\end{aligned}
$$

$$
\begin{aligned}
P_{15} =&\langle x_{12}x_{31} - x_{32}x_{11}, x_{42}x_{11} - x_{41}x_{12}, x_{42}x_{31} - x_{41}x_{32}, x_{44}x_{31} - x_{41}x_{34}, \\
&x_{44}x_{32} - x_{42}x_{34}, x_{13}, x_{21}, x_{22}, x_{23}, x_{24}, x_{33}, x_{43}\rangle \\
&\subset \mathbb{Q}[x_{ij} \mid 1 \le i \le 4, 1 \le j \le 4].
\end{aligned}
$$

$$
\begin{aligned}
P_{16} =&\langle x_{16}x_{27} - x_{17}x_{26}, x_{34}x_{13} - x_{33}x_{14}, x_{37}x_{16} - x_{36}x_{17}, x_{36}x_{27} - x_{37}x_{26}, \\
&x_{12}, x_{15}, x_{21}, x_{22}, x_{23}, x_{24}, x_{25}, x_{32}, x_{35}\rangle \subset \mathbb{Q}[x_{ij} \mid 1 \le i \le 3, 1 \le j \le 7].
\end{aligned}
$$

$$
\begin{aligned}
P_{17} =&\langle e, f, j, z\rangle \subset \mathbb{Q}[b, c, d, e, f, g, h, i, j, z].\\
P_{18} =&\langle c, d, j, z\rangle \subset \mathbb{Q}[b, c, d, e, f, g, h, i, j, z].\\
P_{19} =&\langle -4fec + 3d, b, g, h, z\rangle \subset \mathbb{Q}[b, c, d, e, f, g, h, i, z].\\
P_{20} =&\langle lfdb + 4higc, e, j, m\rangle \subset \mathbb{Q}[b, c, d, e, f, g, h, i, j, k, l, m, z].\\
P_{21} =&\langle c, d, h, j, z\rangle \subset \mathbb{Q}[b, c, d, e, f, g, h, i, j, z].\\
P_{22} =&\langle c, d, g, i, z\rangle \subset \mathbb{Q}[b, c, d, e, f, g, h, i, z].\\
P_{23} =&\langle b, c, d, e, f, g, h, i, z\rangle \subset \mathbb{Q}[b, c, d, e, f, g, h, i, j, k, l, z].\\
P_{24} =&\langle g, i, j, l, z\rangle \subset \mathbb{Q}[b, c, d, e, f, g, h, i, j, k, l, z].\\
P_{25} =&\langle f, g, k, z\rangle \subset \mathbb{Q}[b, c, d, e, f, g, h, i, j, k, l, z].\\
P_{26} =&\langle c, e, g, h, z\rangle \subset \mathbb{Q}[b, c, d, e, f, g, h, z].\\
P_{27} =&\langle c + 4jf, b, d, g, h, k, z\rangle \subset \mathbb{Q}[b, c, d, e, f, g, h, i, j, k, z].
\end{aligned}
$$

6.2 Experiments on Modular Localizations

In this section, we see some naive experiments on SINGULAR [9]. Timings (in seconds) are measured in real time and on a PC with Intel Core i7-8700B CPU with 32GB memory. We see several examples with intermediate coefficient growth. The source code for several algorithms (`modQuotient`, `modSat` and `modDiq`) is open in `https://github.com/IshiharaYuki/moddiq`.

To implement modular algorithms for (double) ideal quotient and saturation, we use the library `modular.lib`. A function `modular` returns a candidate from modular computations by CRT and rational reconstruction. As the optional arguments, the function has `primeTest`, `deleteUnluckyPrimes`, `pTest` and `finalTest`. In this thesis, we implemented `primeTest`, `pTest` and `finalTest` for (double) ideal quotient and saturation. Also, we use Singular implemented functions `quotient` and `sat` to compute $(I : J)$ and $(I : J^{\infty})$ respectively (about computations of ideal quotient and saturation, see [13]). We explain some details of our implementations. First, `modQuotient` computes ideal quotient by modular techniques based on Lemma 5.2.6. Second, `modSat` computes saturation by modular techniques based on Lemma 5.2.12 and Lemma 5.2.13. Third, `diq` computes DIQ by using `quotient` twice and `modDiq` computes DIQ based on Theorem 5.2.8. The function `modDiq` uses `modQuotient` to check the condition that $(I_p(F) : I_p(G)) = \phi_p((I(F) : I(G)) \cap Z_{(p)}[X])$ and $K_{can} \subset (I(F) : (I(F) : I(G)))$ in Theorem 5.2.8. Of course, we can compute DIQ by using `modQuotient` twice.

Here, we use the degree reverse lexicographical ordering (see Example 1.1.2 and `dp` on SINGULAR). We tested our implementation by "cyclic ideal", where $cyclic(n)$ is defined in $\mathbb{Q}[x_1, \ldots, x_n]$ (see the definition in [4]). We let

$$\begin{aligned} P_{28} = \langle & -15x_5 + 16x_6^3 - 60x_6^2 + 225x_6 - 4, 2x_5^2 - 7x_5 + 2x_6^2 - 7x_6 + 28, (4x_6 - 1)x_5 - x_6 + 4, \\ & 4x_1 + x_5 + x_6, 4x_2 + x_5 + x_6, 4x_3 + x_5 + x_6, 4x_4 + x_5 + x_6 \rangle, \\ P_{29} = \langle & x_2^2 + 4x_2 + 1, x_1 + x_2 + 4, x_3 - 1, x_4 - 1, x_5 - 1, x_6 - 1 \rangle \end{aligned}$$

be prime divisors of $cyclic(6)$ and

$$\begin{aligned} Q_{28} = \langle & (-15x_5 + 16x_6^3 - 60x_6^2 + 225x_6 - 4)^2, (2x_5^2 - 7x_5 + 2x_6^2 - 7x_6 + 28)^2, (4x_6 - 1)x_5 - x_6 + 4, \\ & 4x_1 + x_5 + x_6, 4x_2 + x_5 + x_6, 4x_3 + x_5 + x_6, 4x_4 + x_5 + x_6 \rangle \end{aligned}$$

a P_{28}-primary ideal. Also, we let

$$\begin{aligned} I_2 = \langle & 8x^2y^2 + 5xy^3 + 3x^3z + x^2yz, x^5 + 2y^3z^2 + 13y^2z^3 + 5yz^4, 8x^3 + 12y^3 + xz^2, \\ & 7x^2y^4 + 18xy^3z^2 + y^3z^3 \rangle \end{aligned}$$

be a modification of an ideal appearing in [3] and

$$I_3 = \langle xw_{11} - yw_{10}, yw_{12} - zw_{11}, -w_{11}w_{20} + w_{21}w_{10}, -w_{21}w_{12} + w_{22}w_{11} \rangle$$

be $A_{2,3,3}$ (see [27]). As inputs, we used their Gröbner bases.

In Table 6.4, we can see that `modQuotient` is very effective for computation of such ideals. In Table 6.5, we compare timings of computations of saturation in each method. To consider ideals with non-prime components, we take an intersection or products of ideals. We can see that `modSat` is very effective even when multiplicities of target primary components are large. In Table 6.6, we see results of prime divisors checks by DIQ in each method. We can see that modular methods

"double `modQuotient`" and `modDiq` are very efficient, comparing with the rational `diq`. In almost cases in the table, `modDiq` is faster than `modQuotient` since the final test (Theorem 5.2.8) may have some effectiveness for efficient computations.

As a whole, we examined the efficiency of modular techniques for ideal quotients by computational experiments.

ideal quotient	`quotient`	`modQuotient`
$(cyclic(6) : P_{28})$	35.0	11.2
$(cyclic(6) : P_{29})$	15.1	7.65
$(I_2^2 : I_2)$	7.80	0.32
$(I_2^3 : I_2)$	255	7.67
$(I_2^4 : I_2)$	2137	68.8
$(I_2 I_3 : I_3)$	0.88	0.72

Table 6.4: Ideal quotient

saturation	`sat`	`modSat`
$((cyclic(6) \cap Q_{28}) : P_{28}^{\infty})$	86.9	16.4
$(I_2 I_3^2 : I_3^{\infty})$	1264	21.9
$((I_2 \cdot (x^{100}, xy)\rangle : \langle x, y\rangle^{\infty})$	0.33	0.13
$((I_2 \cdot (x^{500}, xy)\rangle : \langle x, y\rangle^{\infty})$	27.3	1.18
$((I_2 \cdot (x^{1000}, xy)\rangle : \langle x, y\rangle^{\infty})$	201	4.25

Table 6.5: Saturation

[ideal, prime divisor]	`diq`	double `modQuotient`	`modDiq`
$[cyclic(6), P_{28}]$	37.0	28.9	17.8
$[cyclic(6), P_{29}]$	15.3	9.36	11.3
$[I_2^3, \langle x, y\rangle]$	13.1	8.96	5.32
$[I_2^4, \langle x, y\rangle]$	254	81.7	41.4
$[I_2^2 I_3, \langle x, y, z\rangle]$	143	80.7	29.1

Table 6.6: Double ideal quotient

Conclusion and Future Works

"Computer Algebra" is an interdisciplinary field of mathematics and computer science. It mainly concerns algebraic computations over the integer ring, the rational field, finite fields, polynomial rings and so on. Computational aspects of Computer Algebra give us variants of application for pure mathematics and applied mathematics by its symbolic computations. This thesis is mainly dedicated to devise efficient methods for operations in polynomial rings, especially *effective localization of ideals* (at a prime ideal).

We provide new algorithms which obtain the particular primary components directly by using Double Ideal Quotient (DIQ) and its variants. We call such algorithms "Local Primary Algorithms(LPAs)". LPAs are based on several generating tools and criteria for primary components with different procedures for two cases; isolated and embedded. For isolated cases, LPAs use the "second saturated quotient" $(I : (I : P^{\infty})^{\infty})$ and its "equidimensional hull" $\mathrm{hull}((I : (I : P^{\infty})^{\infty}))$ to compute the isolated P-primary component of I; while for embedded cases, LPAs use the "equidimensional hull" of $I+P^m$. For improving LPAs, we devise several efficient techniques; $P_G^{[m]}$-products, MIS-hull, and MIS-localization. Also, we present another localization method without DIQ to compare it and LPAs with DIQ. In the computer experiments, we see that LPAs have strong effectiveness by their specialities in almost every cases. In particular, MIS-localization is much effective as an improvement technique for LPAs in many examples (see Table 6.1 and Table 6.3 in Chapter 6). However, its computational behavior is somehow *unstable* (see Figure 6.2, 6.3 in Chapter 6). Hence, we conclude that effectiveness of LPAs depends on ideals and thus, at present, it would be better to apply them in parallel.

To make LPAs more efficiently, we apply *modular techniques* for (double) ideal quotient and saturation. It is well-known that modular techniques are useful to avoid *intermediate coefficient growth* and make rational computations more efficiently. Given ideals I, J, ideal operations $AL(*,*)$ over $\mathbb{Q}[X]$ and $AL_p(*,*)$ over $\mathbb{F}_p[X]$ where p is a prime number, as inputs, we compute $AL(I,J)$ as the output by using modular computations. First, we choose a list of random prime numbers $\mathcal{P}$, which satisfies certain computable condition PRIMETEST. For example, PRIMETEST is to check whether $p \in \mathcal{P}$ is permissible for Gröbner bases of I and J or not. Next, we compute modular operations $H_p = AL_p(I,J)$ for each $p \in \mathcal{P}$. After omitting expected unlucky primes by DELETEUNLUCKYPRIMES, we lift H_p's up to H_{can} by CRT and rational reconstruction. Finally, we check H_{can} is really the correct answer by FINALTEST. If FINALTEST says FALSE, then we enlarge $\mathcal{P}$ and continue from the first step. In this thesis, we introduce new FINALTEST for (double) ideal quotient and saturation. In the computer experiments, we see that modular techniques are effective for such ideal operations.

In future work, to make our LPAs more practical we shall continue to improve it through obtaining timing data for a lot of larger examples. In particular, we need to invent effective algorithms to compute DIQ and MIS-localization. To do it, we can apply our primary component criteria to

probabilistic or inexact methods for primary decomposition, such as numerical ones. Probabilistic or inexact ways may have low computational costs but low accuracy for outputs. Hence, our criteria using DIQ can guarantee their outputs. For example, we are thinking to combine our LPAs and Numerical Primary Decomposition in [20] to compute possible prime divisors and primary components. Of course, it is important to analyze the complexity of LPAs. Meanwhile, we are on the way to implement Associated Check (Algorithm 4, 5) and complete an efficient algorithm of Intermediate Primary Decomposition (IPD) via MIS. We will continue to improve the implementations and extend experiments to other examples. Also, we are thinking about IPD in another way (e.g. using the second saturated quotient) and apply IPD to compute a candidate of a prime divisor.

Bibliography

[1] Atiyah, M.F., MacDonald, I.G.: Introduction to Commutative Algebra. Addison-Wesley Series in Mathematics, Avalon Publishing, New York (1994)

[2] Afzal, D., Kanwal, F., Pfister, G., Steidel, S.: Solving via modular methods. In: Bridging Algebra, Geometry, and Topology, Springer Proceedings in Mathematics & Statistics, **96**, 1-9 (2014)

[3] Arnold, E.: Modular algorithms for computing Gröbner bases. J. Symb. Comput., **35** (4), 403-419 (2003)

[4] Backelin, J., Fröberg, R.: How we prove that there are exactly 924 cyclic 7-roots. In: Proceedings of ISSAC '91, ACM, 103-111 (1991)

[5] Becker, T., Weispfenning, V.: Gröbner Basis: A Computational Approach to Commutative Algebra. Graduate Texts in Mathematics, Springer, New York (1993)

[6] Buchberger, B.: Ein algorithmus zum auffinden der basiselemente des restklassenrings nach einem nulldimensionalen polynomideal. Doctoral Thesis, Mathematical Institute, University of Innsbruck (1965); English translation (Abramson, M.P.): An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. J. Symb. Comput., **41** (3-4), 475-511 (2006)

[7] Böhm, J., Decker, W., Fieker, C., Pfister, G.: The use of bad primes in rational reconstruction. Math. Comput., **84**, 3013-3027 (2015)

[8] Cox, D. A., Little J. B., O'Shea, D.: Ideals, Varieties and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra. Fourth Edition, Undergraduates Texts In Mathematics, Springer, New York (2015)

[9] Decker, W.; Greuel, G.-M.; Pfister, G.; Schönemann, H.: SINGULAR 4-1-2 — A computer algebra system for polynomial computations. `http://www.singular.uni-kl.de` (2019).

[10] Eisenbud, D., Huneke, C., Vasconcelos, W.: Direct methods for primary decomposition. Inventi. Math., **110** (1), 207-235 (1992)

[11] Faugère, J.-C., Gianni, P., Lazard, D., Mora, T.: Efficient computation of zero-dimensional Gröbner bases by change of ordering. J. Symb. Comput., **16** (4), 329-344 (1993)

[12] Gianni, P., Trager, B., Zacharias, G.: Gröbner bases and primary decomposition of polynomial ideals. J. Symb. Comput., **6** (2), 149-167 (1988)

[13] Greuel, G.-M., Pfister, G.: A Singular Introduction to Commutative Algebra. Springer, Heidelberg (2008)

[14] Idrees, N., Pfister, G., Steidel, S.: Parallelization of modular algorithms. J. Symb. Comput., **46** (6), 672-684 (2011)

[15] Ishihara, Y.: Modular techniques for effective localization and double ideal quotient. In Proceedings of ISSAC '20, ACM, 265-272 (2020)

[16] Ishihara, Y., Vaccon, T., Yokoyama, K.: On FGLM algorithms with tropical Gröbner bases. In Proceedings of ISSAC '20, ACM, 257-264 (2020)

[17] Ishihara, Y., Yokoyama, K.: Effective localization using double ideal quotient and its implementation. In: Computer Algebra in Scientific Computing, CASC 2018, LNCS, **11077**, Springer, 272-287 (2018)

[18] Ishihara, Y., Yokoyama, K.: Computation of a primary component of an ideal from its associated prime by effective localization. Communications of Japan Society for Symbolic and Algebraic Computation, **4**, Japan Society for Symbolic and Algebraic Computation, 1-31 (2020)

[19] Kawazoe, T., Noro, M.: Algorithms for computing a primary ideal decomposition without producing intermediate redundant components. J. Symb. Comput., **46** (10), 1158-1172 (2011)

[20] Leykin, A.: Numerical primary decomposition. In Proceedings of ISSAC '08, ACM, 165-172 (2008)

[21] Matsumura, H.: Commutative Algebra. The Benjamin/Cummings Publishing Company, Inc. (1980)

[22] Matzat, B.H., Greuel, G.-M., Hiss, G.: Primary decomposition: algorithms and comparisons. In: Matzat, B.H., Greuel, G.M., Hiss, G. (eds.) Algorithmic Algebra and Number Theory, Springer, Heidelberg, 187-220 (1999)

[23] Noro, M.: Modular algorithms for computing a generating set of the syzygy module. In: Computer Algebra in Scientific Computing, CASC 2009, LNCS, **5743**, Springer, 259-268 (2009)

[24] Noro, M., Yokoyama, K.: Usage of modular techniques for efficient computation of ideal operations. Math.Comput.Sci. **12** (1), 1-32 (2018)

[25] The Risa/Asir developing team: Risa/Asir. A computer algebra system.

`http://www.math.kobe-u.ac.jp/Asir`

[26] Shimoyama, T., Yokoyama, K.: Localization and primary decomposition of polynomial ideals. J. Symb. Comput., **22** (3), 247-277 (1996)

[27] Sturmfels, B.: Solving systems of polynomial equations. In: CBMS Regional Conference Series. American Mathematical Society, no. 97 (2002)

[28] Vasconcelos, W.: Computational Methods in Commutative Algebra and Algebraic Geometry. Algorithms and Computation in Mathematics, **2**, Springer, Heidelberg (2004)

[29] Yokoyama, K.: A note on distinct nilpotency decomposition of polynomial ideals over finite fields, Commentarii mathematici Universitatis Sancti Pauli, **59** (2), Dept. of Mathematics Rikkyo University, 145-164 (2010)