



Effective Localization Using Double Ideal Quotient and Its Implementation

Yuki Ishihara^(✉) and Kazuhiro Yokoyama

Rikkyo University, Tokyo, Japan
{yishihara,kazuhiro}@rikkyo.ac.jp

Abstract. In this paper, we propose a new method for localization of polynomial ideal, which we call “Local Primary Algorithm”. For an ideal I and a prime ideal P , our method computes a P -primary component of I after checking if P is associated with I by using *double ideal quotient* ($I : (I : P)$) and its variants which give us a lot of information about localization of I .

Keywords: Gröbner basis · Primary decomposition · Localization

1 Introduction

In commutative algebra, the operation of “localization by a prime ideal” is well-known as a basic tool. To realize it on computer algebra systems, we propose new effective localization using *double ideal quotient* (DIQ) and its variants for ideals, in a polynomial ring over a field. Here, by the words *localization*, we mean the saturation or the contraction of localized ideals.

It is well-known that the localization of an ideal can be computed through its primary decomposition. In more detail, for an ideal I of a polynomial ring $K[X] = K[x_1, \dots, x_n]$ over a field K and a multiplicatively closed set S in $K[X]$, once a primary decomposition Q of I is known, the localization (i.e. the contraction of localized ideal) of I by S can be computed by $IK[X]_S \cap K[X] = \bigcap_{Q \in \mathcal{Q}, Q \cap S = \emptyset} Q$ (see Remark 3). Algorithms of primary decomposition have been much studied, for example, by [2, 3, 5, 8]. However, in practice, as such primary decomposition tends to be very time-consuming, use of primary decomposition is not an efficient way and we need an efficient *direct* method without primary decomposition. Toward a direct method of localization, for a given ideal I and a prime ideal P , first we provide several criteria for checking if a primary ideal Q can be a P -primary component of I , and then present a direct method named *Local Primary Algorithm* (LPA) which computes a P -primary component of I . Our method applies different procedures for two cases; isolated and embedded. Both cases use *double ideal quotient and its variants* as a tool for generating and checking primary components. Of course, if we know all associated primes disjoint from a multiplicatively closed set, we get its localization without computing other primary components.

For ideals I and J , we call an ideal $(I : (I : J))$ *double ideal quotient* in the paper. Double ideal quotient appears in [10] to check associated primes or compute equidimensional hull, and in [2], to compute equidimensional radical. We survey other properties of double ideal quotient and find that it and its variants have useful information about localization. For instance, for ideals I, J and a primary decomposition \mathcal{Q} of I , a variant of DIQ $(I : (I : J)^\infty)$ coincides with $\bigcap_{Q \in \mathcal{Q}, J \subset IK[X]_{\sqrt{Q}} \cap K[X]} Q$.

To check the practicality of criteria on LPA, we made an implementation on the computer algebra system Risa/Asir [7] and demonstrate the performance in several examples. To evaluate effectiveness coming from its speciality, we compare timings of it to ones of a general algorithm of primary decomposition in Risa/Asir.

For practical implements we devise several efficient techniques for improving our LPA. (For efficient computation of ideal quotient and saturation, see [4, 10]). First, instead of computing the *equidimensional hull* $\text{hull}(I + P^m)$, we use $\text{hull}(I + P_G^{[m]})$ where $P_G^{[m]} = (f_1^m, \dots, f_r^m)$ for some generator $G = \{f_1, \dots, f_r\}$ of P . Second, we use a *maximal independent set* of P for computing $\text{hull}(\overline{Q})$ where \overline{Q} is a P -hull-primary ideal. Since a maximal independent set U of P is one of $I + P^m$, we obtain $\text{hull}(I + P^m) = (I + P^m)K[X]_{K[U]^\times} \cap K[X]$. Moreover, we also use U at the first step of LPA; use $IK[X]_{K[U]^\times} \cap K[X]$ instead of I . By these efficient techniques, our experiment shows certain practicality of our direct localization method.

2 Mathematical Basis

Throughout this paper, we denote a polynomial ring $K[x_1, \dots, x_n]$ by $K[X]$, where K is a computable field (e.g. the rational field \mathbb{Q} or a finite field \mathbb{F}_p) and we denote the set of variables $\{x_1, \dots, x_n\}$ by X . We write $(f_1, \dots, f_t)_{K[X]}$ for the ideal generated by elements f_1, \dots, f_t in $K[X]$. If the ring is obvious, we simply use (f_1, \dots, f_t) . When we simply say I is an ideal, it means the I is an ideal of $K[X]$. Moreover, we denote the radical of I by \sqrt{I} .

2.1 Definition of Primary Decomposition and Localization

Here we give the definition of primary decomposition and that of localization which seem slightly different from *standard* ones. We also give fundamental notions and properties related to localization.

Definition 1. *Let I be an ideal 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} is called a primary decomposition of I if the decomposition $I = \bigcap_{Q \in \mathcal{Q}} Q$ is an irredundant decomposition. 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 and among all prime divisors, 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 $\text{Ass}(I)$ and $\text{Ass}_{\text{iso}}(I)$ the set of all prime divisors of I and the set of all isolated prime divisors respectively.

Definition 2. Let I be an ideal of $K[X]$ and S a multiplicatively closed set in $K[X]$. We denote the set $\{f \in K[X] \mid fs \in I \text{ for some } s \in S\}$ by $IK[X]_S \cap K[X]$, and call it the localization of I with respect to S . For a multiplicatively closed set $K[X] \setminus P$, where P is a prime ideal, we denote simply by $IK[X]_P \cap K[X]$. We assume a multiplicatively closed set S always does not contain 0.

Remark 3. Given a primary decomposition \mathcal{Q} of an ideal I , the localization of I by S is expressed as $\bigcap_{Q \in \mathcal{Q}, Q \cap S = \emptyset} Q$. Moreover, it is also equal to $(I : (\bigcap_{P \in \text{Ass}(I), P \cap S \neq \emptyset} P)^\infty)$. 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 . (We are thinking mainly about cases where S is finitely generated or the complement of a prime ideal. In these cases, we can decide efficiently whether Q and S intersect or not). However, this method is not a direct method since it computes unnecessary primary components or associated primes.

Lemma 4. Let I be an ideal and P a prime divisor of I . 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 $\{Q' \in \mathcal{Q} \mid Q' \cap S \neq \emptyset\} \cup \mathcal{Q}'$ is also a primary decomposition of I . Hence, (B) implies (A).

Definition 5 ([1, Chap. 4]). Let I be an ideal. A subset \mathcal{P} of $\text{Ass}(I)$ is said to be isolated if it satisfies the following condition: for a prime divisor $P' \in \text{Ass}(I)$, if $P' \subset P$ for some $P \in \mathcal{P}$, then $P' \in \mathcal{P}$.

Lemma 6 ([1, Theorem 4.10]). Let I be an ideal and \mathcal{P} an isolated set contained in $\text{Ass}(I)$. For a multiplicatively closed set $S = K[X] \setminus \bigcup_{P \in \mathcal{P}} P$ and a primary decomposition \mathcal{Q} of I , $IK[X]_S \cap K[X] = \bigcap_{Q \in \mathcal{Q}, \sqrt{Q} \in \mathcal{P}} Q$.

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 (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 (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 $IK[X]_S \cap K[X] \subset IK[X]_{\sqrt{Q}} \cap K[X]$. \square

Next we introduce the notion of pseudo-primary ideal.

Definition 8. Let Q be an ideal. We say Q is pseudo-primary if \sqrt{Q} is a prime ideal. In this case, we also say \sqrt{Q} -pseudo-primary.

Definition 9. Let I be an ideal and P an isolated prime divisor of I . For $\mathcal{P} = \{P' \in \text{Ass}(I) \mid P \text{ is the unique isolated prime divisor contained in } P'\}$ and $S = K[X] \setminus \bigcup_{P' \in \mathcal{P}} P'$, we call $\overline{Q} = IK[X]_S \cap K[X]$ the P -pseudo-primary component of I . This definition is consistent with one in [8]. We note that the P -pseudo-primary component is determined uniquely and has the P -isolated primary component of I as component.

Remark 10. Every P -pseudo-primary component of I is a P -pseudo-primary ideal. Let \overline{Q}_P be the P -pseudo-primary component of I . Then $I = \bigcap_{P \in \text{Ass}_{\text{iso}}(I)} \overline{Q}_P \cap I'$ for some I' s.t. $\text{Ass}_{\text{iso}}(I') \cap \text{Ass}_{\text{iso}}(I) = \emptyset$. This decomposition is called a pseudo-primary decomposition in [8], where it is computed by separators from given $\text{Ass}_{\text{iso}}(I)$. Meanwhile, we introduce another method to compute it by using double ideal quotient in Lemma 32.

Definition 11. Let I be an ideal and \mathcal{Q} a primary decomposition of I . We call $\text{hull}(I) = \bigcap_{Q \in \mathcal{Q}, \dim(Q) = \dim(I)} Q$ the equidimensional hull of I . Since every primary component Q satisfying $\dim(Q) = \dim(I)$ is isolated, $\text{hull}(I)$ is determined independently from choice of primary decompositions.

For a given I , $\text{hull}(I)$ can be computed in several manners. For instance, it can be computed by Ext functors [2] or a regular sequence contained in I [10].

Proposition 12 ([2], Theorem 1.1. [10], Proposition 3.41). Let I be an ideal and $u \subset I$ be a c -length regular sequence, where c is the codimension of I . Then $\text{hull}(I) = ((u) : (u) : I) = \text{ann}_{K[X]}(\text{Ext}_{K[X]}^c(K[X]/I, K[X]))$.

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

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

Remark 14. A pseudo-primary ideal is hull-primary.

By the definition of the P -pseudo-primary component of I , it is easy to prove the following lemma.

Lemma 15. Let P be an isolated prime divisor of I and \overline{Q} a P -pseudo-primary component of I . Then, \overline{Q} is a P -hull-primary and $\text{hull}(\overline{Q})$ is the isolated P -primary component of I .

Using Lemma 15 and a variant of double ideal quotient, we generate the isolated P -primary component of I in Sect. 5.

Lemma 16. *Let Q be a primary ideal. Let I and J be ideals. 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, $fg \in IJ \subset Q$ and thus $f \in Q$. □

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

Proof. Let \mathcal{Q} be a primary decomposition of I and $J = \bigcap_{Q' \in \mathcal{Q}, Q' \neq \text{hull}(I)} Q'$. Then $I = \text{hull}(I) \cap J \subset Q$ and $J \not\subset P$. Since Q is P -primary, we obtain $\text{hull}(I) \subset Q$ by Lemma 16. □

Finally, we recall the famous Prime Avoidance Lemma.

Lemma 18 ([1], Proposition 1.11). *(i) Let P_1, \dots, P_n be prime ideals and let I be an ideal contained in $\bigcup_{i=1}^n P_i$. Then, $I \subset P_i$ for some i .*

(ii) Let I_1, \dots, I_n be ideals and let P be a prime ideal containing $\bigcap_{i=1}^n I_i$. Then $P \supset I_i$ for some i . If $P = \bigcap_{i=1}^n I_i$, then $P = I_i$ for some i .

2.2 Fundamental Properties of Ideal Quotient

We introduce fundamental properties of ideal quotient. The first two can be seen in several papers and books ([1], Lemma 4.4. [4], Lemma 4.1.3. [10], a remark before Proposition 3.56). The last two are direct consequences of the first two.

Lemma 19. *Let I and J be ideals, Q a primary ideal and \mathcal{Q} a primary decomposition of I . Then,*

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

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

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

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

3 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:

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

Then, our DIQ is expressed precisely by components of them. The following proposition can be proved directly from Lemma 19. We omit an easy but tedious proof.

Proposition 20. *Let I and J be ideals. Then,*

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

This proposition can be used to prove the following for prime divisors.

Corollary 21 ([10], Corollary 3.4). *Let I be an ideal and P a prime ideal. Then, P belongs to $\text{Ass}(I)$ 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 20, $\sqrt{(I : (I : P))} = \bigcap_{P' \in \text{Ass}(I), P \subset P'} P'$. If $P \in \text{Ass}(I)$, then $\sqrt{(I : (I : P))} = \bigcap_{P' \in \text{Ass}(I), P \subset P'} P' \subset P$. On the other hand, if $P \supset \sqrt{(I : (I : P))}$, then there is $P' \in \text{Ass}(I)$ s.t. $P' \subset P$ and $P' \supset P$. Thus $P = P' \in \text{Ass}(I)$. \square

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

Proposition 22. *Let \mathcal{Q} be a primary decomposition of I . Then,*

$$(I : (I : J)^\infty) = \bigcap_{Q \in \mathcal{Q}, J \subset IK[X]_{\sqrt{Q}} \cap K[X]} Q, \tag{1}$$

$$(I : (I : J^\infty)^\infty) = \bigcap_{Q \in \mathcal{Q}, J \subset \sqrt{IK[X]_{\sqrt{Q}} \cap K[X]}} Q, \tag{2}$$

$$(I : (I : J^\infty)) = \bigcap_{Q \in \mathcal{Q}_2(J)} \left(Q : \bigcap_{Q' \in \mathcal{Q}_1(J)} Q' \right) \cap \bigcap_{Q \in \mathcal{Q}_3(J)} \left(Q : \bigcap_{Q' \in \mathcal{Q}_1(J)} Q' \right). \tag{3}$$

We call them the first saturated quotient, the second saturated quotient, and the third saturated quotient, respectively.

Proof. Here, we give an outline of the proof. The formula (1) 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 19 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) 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 m from the first formula (1), and the following equivalence

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

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

for each $Q \in \mathcal{Q}$. The third formula (3) can be proved directly from Lemma 19. Now, we explain some details. We show (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 18, $\sqrt{Q'} \subset \sqrt{Q}$ for some $Q' \in \mathcal{Q}_1(J) \cup \mathcal{Q}_3(J)$. Since $Q' \subset \sqrt{Q'} \subset \sqrt{Q}$, we obtain $IK[X]_{\sqrt{Q}} \cap K[X] = \bigcap_{Q'' \in \mathcal{Q}, Q'' \subset \sqrt{Q}} Q'' \subset Q'$. However, since $Q' \in \mathcal{Q}_1(J) \cup \mathcal{Q}_3(J)$, we obtain $J \not\subset Q'$ and this contradicts $J \subset IK[X]_{\sqrt{Q}} \cap K[X] \subset Q'$.

Show (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 $Q' \notin \mathcal{Q}_1(J) \cup \mathcal{Q}_3(J)$ 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 (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 $Q' \in \mathcal{Q}_2(J) \cup \mathcal{Q}_3(J)$ for any $Q' \in \mathcal{Q}$ contained in \sqrt{Q} . Thus, we obtain $J^m \subset IK[X]_{\sqrt{Q}} \cap K[X]$. \square

Using the first saturated quotient, we devise criteria for primary component in Sect. 4. The second saturated quotient can be used to isolated prime divisor check and generate an isolated primary component in Sect. 5. The third saturated quotient gives another prime divisor criterion (Criterion 5 in Sect. 4) other than Corollary 19 by the following proposition.

Proposition 23. *Let I and J be ideals. Then $\sqrt{(I : (I : J^\infty))} = \bigcap_{P \in \text{Ass}(I), J \subset P} P$.*

Proof. Let \mathcal{Q} be a primary decomposition of I . By Proposition 22 (3),

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

Since \mathcal{Q} is minimal, we obtain $Q \not\supset \bigcap_{Q' \in \mathcal{Q}_1(J)} Q'$ 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 19,

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

\square

4 Criteria for Primary Component and Prime Divisor

In this section, we present several criteria for primary component which check if a P -primary ideal Q is a primary component of I or not without computing primary decomposition of I based on the first saturated quotient. We first propose a general criterion applicable to any primary ideal. Later, we propose some specialized criteria aiming for isolated primary components and maximal ones. Finally, we add criteria for prime divisors.

4.1 General Primary Component Criterion

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

Definition 24. *Let I and J be ideals. We say that J is saturated quotient invariant of I if $(I : (I : J)^\infty) = J$.*

Any localization is saturated quotient invariant. Conversely, any proper saturated quotient invariant ideal is some localization of I .

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 of I .

Proof. Let \mathcal{Q} be a primary decomposition. Show (A) implies (B). From Proposition 22 (1),

$$(I : (I : IK[X]_S \cap A)^\infty) = \bigcap_{Q \in \mathcal{Q}, IK[X]_S \cap K[X] \subset IK[X]_{\sqrt{Q}} \cap K[X]} Q. \tag{4}$$

By Lemma 7, $IK[X]_S \cap K[X] \subset IK[X]_{\sqrt{Q}} \cap K[X]$ if and only if $Q \cap S = \emptyset$. Thus,

$$\bigcap_{Q \in \mathcal{Q}, IK[X]_S \cap K[X] \subset IK[X]_{\sqrt{Q}} \cap K[X]} Q = \bigcap_{Q \in \mathcal{Q}, Q \cap S = \emptyset} Q, \tag{5}$$

Combining (4), (5) and $IK[X]_S \cap K[X] = \bigcap_{Q \in \mathcal{Q}, Q \cap S = \emptyset} Q$ by Remark 3, we obtain $(I : (I : IK[X]_S \cap A)^\infty) = IK[X]_S \cap K[X]$.

Next, show (B) implies (A). From Proposition 22 (1),

$$(I : (I : J)^\infty) = \bigcap_{J \subset IK[X]_{\sqrt{Q}} \cap K[X]} Q = J. \tag{6}$$

Let $\mathcal{P} = \{\sqrt{Q} \mid Q \in \mathcal{Q}, J \subset IK[X]_{\sqrt{Q}} \cap K[X]\}$. We may assume $\mathcal{P} \neq \emptyset$, otherwise $\mathcal{P} = \emptyset$ and $J = K[X]$. Then \mathcal{P} is *isolated* since if $P' \in \text{Ass}(I)$ and $P' \subset P$ for some $P \in \mathcal{P}$, then $J \subset IK[X]_{P'} \cap K[X] \subset IK[X]_{P'} \cap K[X]$ and $P' \in \mathcal{P}$. Let $S = K[X] \setminus \bigcup_{P \in \mathcal{P}} P$. By Lemma 6, $IK[X]_S \cap K[X] = \bigcap_{Q \in \mathcal{Q}, \sqrt{Q} \in \mathcal{P}} Q = \bigcap_{J \subset IK[X]_{\sqrt{Q}} \cap K[X]} Q$. By (3), we obtain $IK[X]_S \cap K[X] = J$. \square

Based on Lemma 25, we have the following criterion for primary component.

Theorem 26 (Criterion 1). *Let I be an ideal and P a prime divisor of I . For a P -primary ideal Q , if $Q \not\subseteq (I : P^\infty)$, 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 of I .

Proof. Show (A) implies (B). Let \mathcal{Q} be a primary decomposition. Let $\mathcal{P} = \{P' \in \text{Ass}(I) \mid P \not\subseteq P' \text{ or } P' = P\}$ and $S = K[X] \setminus \bigcup_{P' \in \mathcal{P}} P'$. Then S is a multiplicatively closed set and $(I : P^\infty) \cap Q \subset IK[X]_S \cap K[X]$ since $(I : P^\infty) \cap Q = \bigcap_{Q' \in \mathcal{Q}, P \not\subseteq \sqrt{Q'}} Q' \cap Q$. For each $Q' \in \mathcal{Q}$ with $Q' \cap S = \emptyset$, there is $P' \in \mathcal{P}$ such that $\sqrt{Q'} \subset P'$, i.e. $\sqrt{Q'} \in \mathcal{P}$. 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 25, $IK[X]_S \cap K[X]$ is saturated quotient invariant of I .

Show (B) implies (A). By Lemma 25, 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, $Q \not\subseteq (I : P^\infty)$ 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,

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

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

4.2 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.

Criterion for Isolated Primary Component: If Q is a primary ideal whose radical is an isolated divisor P of an ideal I , then we don't need to compute $(I : P^\infty)$ since the P -primary component of I is the localization of I by P .

Theorem 27 (Criterion 2). *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 (A) implies (B). Let $S = K[X] \setminus P$. By Lemma 25, $Q = IK[X]_S \cap K[X]$ is saturated quotient invariant of I and thus $(I : (I : Q)^\infty) = Q$. Next, we show (B) implies (A). By Lemma 25, 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. □

Criterion for Maximal Primary Component: Each isolated prime divisor is minimal in $\text{Ass}(I)$. On the contrary, we consider “maximal prime divisor” and propose the following criterion for it.

Definition 28. Let P be a prime divisor of I . We say P is maximal if there is no prime divisor P' of I containing P properly.

Theorem 29 (Criterion 3). Let I be an ideal and P a maximal prime divisor of I . For 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 (A) implies (B). Let \mathcal{Q} be a primary decomposition of I with $Q \in \mathcal{Q}$. Since P is maximal in $\text{Ass}(I)$, $(I : P^\infty) = \bigcap_{Q' \in \mathcal{Q}, \sqrt{Q'} \not\supseteq P} Q' = \bigcap_{Q' \in \mathcal{Q}, Q' \neq Q} Q'$. Thus, $(I : P^\infty) \cap Q = \bigcap_{Q' \in \mathcal{Q}, Q' \neq Q} Q' \cap Q = I$. Next, we show (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 . \square

Criterion for Another General Primary Component: The general case can be reduced to maximal case via localization by maximal independent set (See [4] the definition of maximal independent and its computation). Letting $S = K[U]^\times = K[U] \setminus \{0\}$, we obtain the following as a special case of Lemma 4.

Theorem 30 (Criterion 4). Let I be an ideal and P a prime divisor of I . If U is a maximal independent set of P in X 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 $IK[X]_{K[U]^\times} \cap K[X]$.

4.3 Additional Criterion for Prime Divisor

Here, we add a criterion for prime divisor based on the third saturated quotient.

Theorem 31 (Criterion 5). Let I be an ideal and P a prime ideal. Then, the following conditions are equivalent.

- (A) $P \in \text{Ass}(I)$.
- (B) $P \supset (I : (I : P))$.
- (C) $P \supset (I : (I : P^\infty))$.

Proof. By Corollary 21, (A) is equivalent to (B). By Proposition 23, $\sqrt{(I : (I : P))} = \sqrt{(I : (I : P^\infty))} = \bigcap_{P' \in \text{Ass}(I), P \subset P'} P'$. Thus, equivalence between (A) and (C) is proved in a similar way to Corollary 21. \square

Next, we devise criteria for isolated prime divisor based on the second saturated quotient.

Lemma 32. *Let I be an ideal and P an isolated prime divisor of I . If \overline{Q} is the P -pseudo-primary component of I , then $(I : (I : P^\infty)^\infty) = \overline{Q}$.*

Proof. Let \mathcal{Q} be a primary decomposition of I . By Proposition 22 (2),

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

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

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

However, this implies $P \subset P'$ and contradicts that P' is isolated. It is easy to prove that (1-b) implies (1-a). □

Theorem 33 (Criterion 6). *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 (A) implies (B). By Lemma 32, $(I : (I : P^\infty)^\infty) = \overline{Q} \neq K[X]$. Show (B) implies (A). By Proposition 22 (2),

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

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 33 directly induces the following.

Corollary 34 (Criterion 7). *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 $(I : (I : P^\infty)^\infty) = K[X]$.

5 Local Primary Algorithm

In this section, we devise Local Primary Algorithm (LPA) which computes P -primary component of I . Our method applies different procedures for two cases; isolated and embedded. Algorithm 1 shows the outline of LPA. Its termination comes from Proposition 35. We remark that, for given prime divisors disjoint from a multiplicatively closed set S , we can compute all primary components disjoint from S by LPA. Then their intersection gives the localization by S .

5.1 Generating Primary Component

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

Proposition 35 ([2], Sect. 4. [6], 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 , $\text{hull}(I + P^m)$ is a P -primary component appearing in a primary decomposition of I .*

We can use Criteria for Primary Component to check m is large enough or not. If P is an isolated prime divisor, then the component is computed directly by using the second saturated quotient. By Lemmas 15 and 32, we obtain the following theorem.

Theorem 36. *Let I be an ideal and P an isolated prime divisor of I . Then $\text{hull}((I : (I : P^\infty)^\infty))$ is the isolated P -primary component of I .*

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

```

1: if  $P$  is a prime divisor of  $I$  (Criterion 5) then
2:   if  $P$  is isolated (Criteria 6,7) then
3:      $\bar{Q} \leftarrow$  the  $P$ -pseudo-primary component of  $I$  (Lemma 32)
4:      $Q \leftarrow \text{hull}(\bar{Q})$  (Theorem 36)
5:     return  $Q$  is the isolated  $P$  primary component
6:   else
7:      $m \leftarrow 1$ 
8:     while  $Q$  is not primary component of  $I$  (Criteria 1,3,4) do
9:        $\bar{Q} \leftarrow$  a  $P$ -hull-primary ideal related to  $m$  (Proposition 35, Lemma 38)
10:       $Q \leftarrow \text{hull}(\bar{Q})$ 
11:       $m \leftarrow m + 1$ 
12:    end while
13:    return  $Q$  is an embedded  $P$ -primary component
14:  end if
15: else
16:   return "  $P$  is not a prime divisor"
17: end if

```

5.2 Techniques for Improving LPA

We introduce a practical technique for implementing LPA.

5.3 Another Way of Generating Primary Component

Let $G = \{f_1, \dots, f_r\}$ be a generator of P . Usually we take $\{f_1^{e_1} f_2^{e_2} \dots f_r^{e_r} \mid e_1 + \dots + e_r = m\}$ 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 $\text{hull}(I+P^m)$ when m becomes large. To avoid the explosion of the number of the generator, we can use $P_G^{[m]} = (f_1^m, \dots, f_r^m)$ instead.

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 $(\mathcal{Q} \setminus \{Q\}) \cup \{\text{hull}(Q')\}$ is another primary decomposition of I .*

Proof. By Lemma 17, we obtain $I \subset Q' \subset \text{hull}(Q') \subset Q$. Since $I \cap \text{hull}(Q') = I$ and $Q \cap \text{hull}(Q') = \text{hull}(Q')$, we obtain

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

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

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

Proof. As $\sqrt{I + P} = \sqrt{I + P_G^{[m]}} = P$, $I + P_G^{[m]}$ is P -hull-primary. By Theorem 35, $\text{hull}(I + P^m)$ is a P -primary component of I for a sufficiently large m . Since $I \subset I + P_G^{[m]} \subset I + P^m \subset \text{hull}(I + P^m)$, $\text{hull}(I + P_G^{[m]})$ is a P -primary component by Lemma 37. \square

5.4 Equidimensional Hull Computation with MIS

Next, we devise another computation of $\text{hull}(I + P^m)$ based on *maximal independent set* (MIS) which is much efficient than computations based on Proposition 12. Similarly, by this technique we can replace I with $IK[X]_{K[U]^\times} \cap K[X]$ at the first step of LPA.

Lemma 39. *Let I be a P -hull-primary ideal. For a maximal independent set U of P , $\text{hull}(I) = IK[X]_{K[U]^\times} \cap K[X]$.*

Proof. Let \mathcal{Q} be a primary decomposition of I . Then, $\text{hull}(I)$ is the unique primary component disjoint from $K[U]^\times$. Thus,

$$IK[X]_{K[U]^\times} \cap K[X] = \bigcap_{Q \in \mathcal{Q}, Q \cap K[U]^\times = \emptyset} Q = \text{hull}(I).$$

\square

6 Experiments

We made a preliminary implementation on a computer algebra system Risa/Asir [7] and apply it to several examples as naive experiments. Here we show some typical examples. Timings are measured on a PC with Xeon E5-2650 CPU.

First, we see an ideal whose embedded primary components are hard to compute. Let $I_1(n) = (x^2) \cap (x^4, y) \cap (x^3, y^3, (z + 1)^n + 1)$. If n is considerably large, it is difficult to compute a full primary decomposition of $I_1(n)$ though the isolated divisor (x) can be detected pretty easily. We apply Local Primary Algorithm (LPA) for this example to compute the isolated primary component for $P_1 = (x)$. We also see another example which is more valuable for mathematics. An ideal $A_{k,m,n}$ is defined in [9] and its primary decomposition has important meanings in Computer Algebra for Statistics. We consider an isolated prime divisor $P_2 = (x_{13}, x_{23}, x_{33}, x_{43})$ of $A_{3,4,5}$ in $\mathbb{Q}[x_{ij} \mid 1 \leq i \leq 4, 1 \leq j \leq 5]$. In Table 1, we can see LPA has certain effectiveness by its speciality comparing a full primary decomposition function `noro_pd.syci_dec`. From Proposition 12, we also use double ideal quotient to compute equidimensional hull.

Table 1. Local primary algorithm (isolated)

Algorithm	$I_1(100)$	$I_1(200)$	$I_1(300)$	$I_1(400)$	$I_1(500)$	$A_{3,4,5}/P_2$
<code>noro_pd.syci_dec</code>	0.36	15.6	88.3	289	96.0	>3600
LPA	0.02	0.04	0.07	0.11	0.14	14.3

Second, we consider embedded prime divisors; $P_3 = (x_{12}x_{31} - x_{32}x_{11}, x_{42}x_{11} - x_{41}x_{12}, x_{42}x_{31} - x_{41}x_{32}, x_{44}x_{31} - x_{41}x_{34}, x_{44}x_{32} - x_{42}x_{34}, x_{13}, x_{21}, x_{22}, x_{23}, x_{24}, x_{33}, x_{43})$ of $A_{2,4,4}$ in $\mathbb{Q}[x_{ij} \mid 1 \leq i \leq 4, 1 \leq j \leq 4]$ and $P_4 = (x_{16}x_{27} - x_{17}x_{26}, x_{34}x_{13} - x_{33}x_{14}, x_{37}x_{16} - x_{36}x_{17}, x_{36}x_{27} - x_{37}x_{26}, x_{12}, x_{15}, x_{21}, x_{22}, x_{23}, x_{24}, x_{25}, x_{32}, x_{35})$ of $A_{2,3,7}$ in $\mathbb{Q}[x_{ij} \mid 1 \leq i \leq 3, 1 \leq j \leq 7]$. In Table 2, LPA-Pm is an implementation based on Lemma 38 and LPA-MIS is one from Lemma 39 and Criteria 3, 4. Both methods are implemented in LPA-(Pm+MIS). The primitive LPA is not practical since the cost of computing $\text{hull}(I + P^m)$ is very high. On the other hand, we can see LPA-(Pm+MIS) has good effectiveness by its speciality comparing a full primary decomposition function `noro_pd.syci_dec`.

Table 2. Local primary algorithm (embedded) and its improvement

Algorithm	$A_{2,4,4}/P_3$	$A_{2,3,7}/P_4$
<code>noro_pd.syci_dec</code>	3.11	34.8
LPA	>3600	168
LPA-Pm	4.75	29.1
LPA-MIS	0.58	0.38
LPA-(Pm + MIS)	0.15	0.08

7 Conclusion and Future Work

In commutative algebra, the operation of “localization by a prime ideal” is well-known as a basic tool. However, its computation through primary decomposition is very difficult. Thus, we devise a new effective localization *Local Primary Algorithm* (LPA) using Double Ideal Quotient (DIQ) and its variants without computing unnecessary primary components for localization. For our construction of LPA, we devise several criteria for primary component based on DIQ and its variants. We take preliminary benchmarks for some examples to examine certain effectiveness of LPA coming from its speciality. To make our LPA very practical we shall continue to improve it through obtaining timing data for a lot of larger examples.

In future work, we are finding a way to compute “sample points” of prime divisors. For localization it does not need all divisors; it is enough to find $f_P \in P \cap S$ for each prime divisor P with $P \cap S \neq \emptyset$ and we obtain $IK[X]_S \cap K[X] = (I : (\prod_{P \cap S \neq \emptyset} f_P)^\infty)$. Another work is to apply our primary component criteria to *probabilistic or inexact* methods for primary decomposition, such as numerical ones. Probabilistic or inexact ways have low computational costs, however, they have low accuracy for outputs. Hence, our criterion using double ideal quotient may help to guarantee their outputs. Finally, localization in general setting, that is localization by a prime ideal not necessary associated is interesting work.

Acknowledgment. The authors would like to thank the referees for their helpful comments to improve the presentation of this paper. The authors are also grateful to Masayuki Noro for technical assistance with the computer experiments and coding on Risa/Asir.

References

1. Atiyah, M.F., MacDonald, I.G.: Introduction to Commutative Algebra. Addison-Wesley Series in Mathematics. Avalon Publishing, New York (1994)
2. Eisenbud, D., Huneke, C., Vasconcelos, W.: Direct methods for primary decomposition. *Inventi. Math.* **110**(1), 207–235 (1992)
3. Gianni, P., Trager, B., Zacharias, G.: Gröbner bases and primary decomposition of polynomial ideals. *J. Symb. Comput.* **6**(2), 149–167 (1988)
4. Greuel, G.-M., Pfister, G.: A Singular Introduction to Commutative Algebra. Springer, Heidelberg (2002). <https://doi.org/10.1007/978-3-662-04963-1>
5. Kawazoe, T., Noro, M.: Algorithms for computing a primary ideal decomposition without producing intermediate redundant components. *J. Symb. Comput.* **46**(10), 1158–1172 (2011)
6. 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*, pp. 187–220. Springer, Heidelberg (1999). https://doi.org/10.1007/978-3-642-59932-3_10
7. The Risa/Asir developing team: Risa/Asir. A computer algebra system. <http://www.math.kobe-u.ac.jp/Asir>

8. Shimoyama, T., Yokoyama, K.: Localization and primary decomposition of polynomial ideals. *J. Symb. Comput.* **22**(3), 247–277 (1996)
9. Sturmfels, B.: Solving systems of polynomial equations. In: *CBMS Regional Conference Series*. American Mathematical Society, no. 97 (2002)
10. Vasconcelos, W.: *Computational Methods in Commutative Algebra and Algebraic Geometry. Algorithms and Computation in Mathematics*. Springer, Heidelberg (2004)