J. Symbolic Computation (1996) **22**, 247–277

Localization and Primary Decomposition of Polynomial Ideals

TAKESHI SHIMOYAMA AND KAZUHIRO YOKOYAMA†

FUJITSU LABORATORIES, ISIS
140 Miyamoto, Numazu-shi, Shizuoka 410-03, Japan

(Received 4 October 1994)

In this paper, we propose a new method for primary decomposition of a polynomial ideal, not necessarily zero-dimensional, and report on a detailed study for its practical implementation. In our method, we introduce two key techniques, *effective localization* and *fast elimination of redundant components*, by which we can get a good performance for several examples. The performance of our method is examined by comparison with other existing methods based on practical experiments.

© 1996 Academic Press Limited

1. Introduction

In commutative algebra, the technique of "localization by a prime ideal" is well-known as a basic tool. For realization of this technique on computer algebra systems, we propose *effective localization* and apply it to the computation of primary decompositions of ideals, not necessarily zero-dimensional, in a polynomial ring over the rational number field.

The theory of primary decomposition of ideals in noetherian rings is very classical and much work was done for its computation. After the discovery of Gröbner bases (Buchberger, 1965, 1985), concrete algorithmic methods applicable to actual problems were given based on Gröbner bases techniques. Lazard (1985), Kredel (1987) and others showed algorithms for zero-dimensional ideals. Gianni *et al.* (1988), Rutman (1992), Becker & Weispfenning (1993) showed algorithms for non-zero-dimensional ideals by extending algorithms for the zero-dimensional case. Eisenbud *et al.* (1992) proposed another approach, where for a given ideal its prime divisors are computed at the beginning and a primary decomposition is obtained by localization with respect to those prime divisors. However, as far as the authors know, there is no work on the complexity of algorithms for non-zero dimensional ideals and little was done on complete implementation and experiments.

In this paper we propose a new method aimed at practical computation and we discuss performance based on experiments in our complete implementation.

One of the key ideas of our method is that, instead of *direct* localization, we employ *effective* localization by an isolated prime divisor of the given ideal and by this localization

† E-mail: {shimo,momoko}@iias.flab.fujitsu.co.jp

0747–7171/96/090247 + 31 $25.00/0 © 1996 Academic Press Limited

we extract each isolated primary component of the given ideal. This idea is realized by the following three parts:

(1) prime decomposition of the radical of a given ideal;

(2) decomposition of the ideal into *pseudo-primary ideals*;

(3) extraction of prime components from pseudo-primary ideals.

Here a *pseudo-primary ideal* is an ideal whose radical is a prime ideal. By these three steps, we can compute every isolated primary components of the given ideal. As already mentioned, Eisenbud *et al.* (1992) also used localization. However, their localization techniques are quite different from ours from a practical computational point of view. Their localization technique can compute the "localization of an ideal I at an ideal J" but it involves computation of extensions of syzygies. In contrast, the localization of the given ideal at its isolated prime divisor can be computed by the combination of two other easily computable localizations.

By performing effective localization, we can compute embedded components. In this step we have to eliminate *redundant* components. Our second key idea is *fast elimination of redundant components* which deals with this problem. By *fast elimination of redundant components* we can avoid unnecessary effective localizations and compute *shortest irredundant primary decompositions*. We note that many existing papers, except Alonso *et al.* (1990), paid little attention to the property *shortest irredundancy* or gave very simple consideration, that is, *reduction* to the computation of intersections of ideals.

In the method, the computation of prime decompositions of radicals is one of the crucial steps. Since it is independent of other parts, we can adopt any efficient algorithm for it. By theoretical analysis of the proposed method, we found that we required two different kinds of prime decompositions of radicals, one for arbitrary ideals and the other for ideals in special form. To achieve a practical implementation we propose a new method for ideals in special form. For the prime decomposition of radicals for arbitrary ideals we apply a *practical* modification of the method given by Becker & Weispfenning (1993) based on Gianni *et al.*'s approach.

We do not give the computational complexity of the proposed method. Instead we give a certain theoretical analysis of it by which we obtain *fast elimination of redundant components* and succeed in giving a bound of the number of required *effective localizations*. To demonstrate the performance of the method, we implemented the proposed method and the method given by Becker & Weispfenning (1993) (as the most recent and efficient one based on Gianni *et al.*'s approach) in the computer algebra system Risa/Asir (Noro & Takeshima, 1992) and compared the methods in several examples. Moreover, we also made a comparison with an existing implementation given by Gräbe (1995) based on Gianni *et al.*'s approach. For these examples the proposed method seems to be much more efficient than the methods based on Gianni *et al.*'s approach, especially for examples with embedded components. Although our comparison with a limited number of examples cannot prove the superiority of the proposed method, it may suggest a certain quality of the proposed method and our implementation for practical computation. Our study of the practical implementation and the proposed criteria for irredundant components also seems very useful for improving other methods.

2. Mathematical Basis

Throughout this paper, we denote the polynomial ring $\mathbb{Q}[x_1, \ldots, x_n]$ by R, where $\mathbb{Q}$ is the rational number field, and we denote the set of variables $\{x_1, \ldots, x_n\}$ by X. We write $Id(f_1, \ldots, f_t)$ for the ideal generated by elements $f_1, \ldots, f_t$ in R, and $(I : f)$ for the quotient ideal of an ideal I by an element f in R. 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 localization which seem slightly different from "standard" definitions. In the Appendix, we provide other necessary notions and known results which can be found in several books (Zariski & Samuel, 1958/60; Nagata, 1962; Atiyah & MacDonald, 1969; Becker & Weispfenning, 1993).

Definition 2.1. (see details in Definition A.1) *Let I be an ideal of R. A set $\mathcal{Q}$ of primary ideals is called a* general primary decomposition *of I if $I = \cap_{Q \in \mathcal{Q}} Q$. A general primary decomposition $\mathcal{Q}$ is called a* primary decomposition *of I if the decomposition $I = \cap_{Q \in \mathcal{Q}} Q$ is a shortest irredundant decomposition. 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. We denote by* $\mathrm{Ass}(I)$ *and* $\mathrm{Ass}_{iso}(I)$ *the set of all prime divisors of I and that of all isolated prime divisors of I, respectively.*

We note that $\mathrm{Ass}(I)$ and $\mathrm{Ass}_{iso}(I)$ are independent of the particular primary decomposition and $\mathrm{Ass}_{iso}(I) = \mathrm{Ass}(\sqrt{I})$.

Our goal is to compute a *primary decomposition* for a given ideal. We note that from a general primary decomposition, we can obtain a primary decomposition by eliminating redundant components and combining components associated with the same prime ideal. (See Remark A.1.) Next we define *localization of ideals* which corresponds to *saturation* or *contraction of the localized ideals.*

Definition 2.2. *Let I be an ideal of R and T a multiplicatively closed set in R. We denote the set $\{a \in R \mid ab \in I \text{ for some } b \in T \setminus \{0\}\}$ by $IR_T \cap R$, and call it the* localization of I with respect to T. *For a finite set S in R and an element f we denote $IR_{\langle S \rangle} \cap R$ and $IR_{\langle f \rangle} \cap R$ simply by $IR_S \cap R$ and $IR_f \cap R$, respectively, where $\langle S \rangle$ is the multiplicatively closed set generated by S and $\langle f \rangle$ is that by f. For a multiplicatively closed set $R \setminus P$, where P is a prime ideal, we denote $IR_{R \setminus P} \cap R$ simply by $IR_P \cap R$.*

2.2. Pseudo-primary decomposition and extraction

We introduce *pseudo-primary ideal*, which may be a certain generalization of *symbolic powers*, and give two decompositions *pseudo-primary decomposition* and *extraction.*

Definition 2.3. *An ideal I of R is called a* pseudo-primary ideal *if $\sqrt{I}$ has a unique prime component, that is, $\sqrt{I}$ is a prime ideal.*

PROPOSITION 2.4. *Let I be an ideal of R which is not a pseudo-primary ideal, $P_1, \ldots, P_r$ all isolated prime divisor of I, and $\mathcal{Q}$ a primary decomposition of I. Suppose that there are finite subsets $S_1, \ldots, S_r$ in R which satisfy the following conditions:*

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

Then the following hold.

(1) *The ideal $IR_{S_i} \cap R$ is a pseudo-primary ideal whose radical is P_i.*
(2) *Set $\mathcal{Q}_i = \{Q \in \mathcal{Q} \mid \sqrt{Q} \cap S_i = \emptyset\}$. Then $\mathcal{Q}_i$ is a primary decomposition of $IR_{S_i} \cap R$.*

PROOF. Let $\mathcal{P}_i = \{P \in \mathrm{Ass}(I) \mid P \cap S_i = \emptyset\}$. Proposition 4.9 in Atiyah & MacDonald (1969) (Lemma A.5) implies (2) directly. Each embedded prime divisor of I contains at least one isolated prime divisor. From the condition (A) each prime divisor belonging to $\mathcal{P}_i$ contains none of P_j for $j \neq i$ and hence it contains P_i. This implies (1). □

DEFINITION 2.5. *For an ideal I, each S_i which satisfies the condition* (A) *in Proposition* 2.4 *is called a* separator *of I with respect to P_i, and the set $\{S_1, \ldots, S_r\}$ is called a* system of separators *of I.*

COROLLARY 2.6. *We use the same notations as in Proposition* 2.4. *Then*

(1) *$\mathcal{Q}_1, \ldots, \mathcal{Q}_r$ are disjoint and their associated primes sets $\mathcal{P}_1, \ldots, \mathcal{P}_r$ are also disjoint.*
(2) *Each pseudo-primary component is determined by I and a system of separators, i.e, it is independent of the particular primary decomposition.*

Now we present *pseudo-primary decomposition*.

THEOREM 2.7. *We use the same notations as in Proposition* 2.4. *For each i, let $\overline{Q}_i = IR_{S_i} \cap R$, $s_i = \prod_{s \in S_i} s$, and k_i an integer such that $(I : s_i^{k_i}) = IR_{s_i} \cap R$. Then*

$$I = \overline{Q}_1 \cap \cdots \cap \overline{Q}_r \cap I', \tag{B}$$

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

PROOF. The existence of such an integer k_i follows from the fact that an ascending chain of ideals $\{(I : s_i) \subset (I : s_i^2) \subset \cdots\}$ is finite. By Lemma A.2 (4), $(I : s_i^{k_i}) = IR_{s_i} \cap R = IR_{S_i} \cap R = \overline{Q}_i$. The following claims prove the decomposition (B).

CLAIM 1. *$s_j^{k_j} \in (I : s_i^{k_i})$ when $i \neq j$.*

Consider a component Q in $\mathcal{Q}_i$. Then, for each $j \neq i$ $(Q : s_j^{k_j})$ contains $\overline{Q}_j$, since $\overline{Q}_j = (I : s_j^{k_j})$ and Q contains I. If $(Q : s_j^{k_j}) \neq R$, i.e. Q does not contain $s_j^{k_j}$, then $(Q : s_j^{k_j})$ is a proper ideal and moreover, it is a $\sqrt{Q}$-associated primary ideal (see Lemma 4.4 in Atiyah & MacDonald, 1969). Then by considering radicals, its associated prime $\sqrt{Q}$ contains $P_j = \sqrt{\overline{Q}_j}$. Since P_j meets S_i, $\sqrt{Q}$ meets S_i. This contradicts the fact that Q belongs to $\mathcal{Q}_i$. Thus, each component Q in $\mathcal{Q}_i$ contains $s_j^{k_j}$ for $i \neq j$. This implies that $(I : s_i^{k_i}) = \overline{Q}_i$ contains $s_j^{k_j}$ for $j \neq i$.

CLAIM 2. $I = (I : s_1^{k_1}) \cap (I : s_2^{k_2}) \cap \cdots \cap (I : s_r^{k_r}) \cap Id(I, s_1^{k_1}, \ldots, s_r^{k_r})$.

By Proposition 8.95 in Becker & Weispfenning (1993) (Lemma A.3), $I = (I : s_i^{k_i}) \cap Id(I, s_i^{k_i})$ for every i. Substituting I with $(I : s_2^{k_2}) \cap Id(I, s_2^{k_2})$ in $Id(I, s_1^{k_1})$, we have

$$I = (I : s_1^{k_1}) \cap Id(\{(I : s_2^{k_2}) \cap Id(I, s_2^{k_2})\}, s_1^{k_1}).$$

From Claim 1, the element $s_1^{k_1}$ belongs to the ideal $(I : s_2^{k_2})$. By Lemma A.2 (3),

$$Id(\{(I : s_2^{k_2}) \cap Id(I, s_2^{k_2})\}, s_1^{k_1}) = (I : s_2^{k_2}) \cap Id(I, s_1^{k_1}, s_2^{k_2}).$$

Thus,

$$I = (I : s_1^{k_1}) \cap (I : s_2^{k_2}) \cap Id(I, s_1^{k_1}, s_2^{k_2}).$$

By repeating this operation for $r - 1$ times, we get the statement of Claim 2.

Finally we show that $\dim(I') < \dim(I)$ when $I' \neq R$. We assume $I' \neq R$. For each isolated prime divisor P' of I', P' contains $\sqrt{I'}$ and so it also contains $\sqrt{I} = P_1 \cap \cdots \cap P_r$. Then P' contains some P_i. (See Proposition 1.11 in Atiyah & MacDonald, 1969.) Moreover, since $s_i \notin P_i$, we have $\sqrt{I'} \not\subset P_i$ which implies $P_i \neq P'$. From this we have $\dim(P') < \dim(I)$ as $\dim(I) = \max\{\dim(P_1), \ldots, \dim(P_r)\}$. Since this inequality holds for every isolated prime divisor P' of I', we obtain $\dim(I') < \dim(I)$. □

DEFINITION 2.8. *Let I be an ideal of R. The decomposition* (B) *in Theorem* 2.7 *is called a* pseudo-primary decomposition. *Each $\overline{Q}_i$ is called a* pseudo-primary component *of I, and I' is called* the remaining component *in pseudo-primary decomposition.*

COROLLARY 2.9. *We use the same notations as in Theorem* 2.7. *Then we have* $\sqrt{I'} = \sqrt{Id(P_1, s_1)} \cap \cdots \cap \sqrt{Id(P_r, s_r)}$.

PROOF. By using Lemma A.2 (5), we have $\sqrt{Id(I, s_1^{k_1}, \ldots, s_r^{k_r})} = \sqrt{Id(\sqrt{I}, s_1, \ldots, s_r)}$. As $\sqrt{I} = \cap_{i=1}^r P_i$, we obtain $\sqrt{Id(I, s_1^{k_1}, \ldots, s_r^{k_r})} = \sqrt{Id(\cap_{i=1}^r P_i, s_1, \ldots, s_r)}$.

Next we show $\sqrt{Id(\cap_{i=1}^r P_i, s_1, \ldots, s_r)} = \cap_{i=1}^r \sqrt{Id(P_i, s_i)}$. Let $P^{(i)} = \cap_{j=i}^r P_j$ for $1 \leq i \leq r$. Since P_i contains s_j for $j \neq i$, $P^{(2)} = \cap_{i=2}^r P_i$ contains s_1 and P_1 contains s_j for $j \neq 1$. By Lemma A.2 (3) we have

$$\begin{aligned} Id(P_1 \cap P^{(2)}, s_1, \ldots, s_r) &= Id(Id(P_1 \cap P^{(2)}, s_1), s_2, \ldots, s_r) \\ &= Id(P_1, s_1) \cap Id(P^{(2)}, s_2, \ldots, s_r). \end{aligned}$$

Repeating this, we finally obtain $Id(P^{(1)}, s_1, \ldots, s_r) = \cap_{i=1}^r Id(P_i, s_i)$. By Lemma A.2 (5), $\sqrt{\cap_{i=1}^r Id(P_i, s_i)} = \cap_{i=1}^r \sqrt{Id(P_i, s_i)}$. Thus we have the corollary. □

COROLLARY 2.10. *When the ideal I has no embedded primary components, the pseudo-primary decomposition except I' is the primary decomposition of I.*

Next we show that the isolated primary component of a given pseudo-primary ideal can be extracted by *localization* technique.

PROPOSITION 2.11. *Let I be a pseudo-primary ideal with radical P and let Q be its unique isolated primary component. Suppose that a subset U of X is a maximally independent set modulo P. Then $Q = I\mathbb{Q}(U)[X \setminus U] \cap R$.*

PROOF. We denote $\mathbb{Q}(U)[X \setminus U]$ by $\mathbb{Q}_U$ for simplicity. We note that $J\mathbb{Q}_U \cap R = JR_{\mathbb{Q}[U]^*} \cap R$ for every ideal J, where $\mathbb{Q}[U]^* = \mathbb{Q}[U] \setminus \{0\}$. Fix a primary decomposition $\{Q, Q_1, \ldots, Q_r\}$ of I. Since U is a maximally independent set modulo P, $P \cap \mathbb{Q}[U]^* = \emptyset$ and $|U| = \dim(P)$ (see Lemma A.11). This implies $Q\mathbb{Q}_U \cap R = Q$ by Proposition 4.8 in Atiyah & MacDonald (1969) (Lemma A.4). On the other hand, for each Q_i, $\sqrt{Q_i}$ contains P properly and so $|U| = \dim P > \dim \sqrt{Q_i}$. Therefore, U is not an independent set modulo $\sqrt{Q_i}$ and $\sqrt{Q_i} \cap \mathbb{Q}[U]^* \neq \emptyset$. Then we obtain $Q_i\mathbb{Q}_U \cap R = R$ and $I\mathbb{Q}_U \cap R = (Q\mathbb{Q}_U \cap R) \cap (\cap_{i=1}^{r}(Q_i\mathbb{Q}_U \cap R)) = Q$. (See Lemma A.5.) □

THEOREM 2.12. *We use the same notation as in Proposition* 2.11. *Let f be an element of R as in Proposition* 8.94 *in Becker & Weispfenning* (1993) *(Lemma* A.8*) with respect to U, k an integer such that $IR_f \cap R = (I : f^k)$ and I' an ideal $Id(I, f^k)$. Then $Q = IR_f \cap R$ and*

$$I = Q \cap I'. \tag{C}$$

Moreover, either $I' = R$ or $\dim(I) > \dim(I')$ holds.

PROOF. By Lemma A.3, $I = (I : f^k) \cap Id(I, f^k)$. From Lemma A.8 and Proposition 2.11, $Q = I\mathbb{Q}(U)[X \setminus U] \cap R = IR_f \cap R = (I : f^k)$. Thus we have $I = Q \cap I'$.

Now we show that $\dim(I') < \dim(I)$ if $I' \neq R$. Since $I \subset I'$ and $f^k \notin P$, we have $P = \sqrt{I} \subset \sqrt{I'}$ and $P \neq \sqrt{I'}$. From this we have $\dim(I) = \dim(P) > \dim(I')$. □

DEFINITION 2.13. *Let I be a pseudo-primary ideal with radical P. The decomposition* (C) *in Theorem* 2.12 *is called an* extraction *of Q from I and I' is called the* remaining component *in extraction. The element f is called the* extractor *associated with P.*

COROLLARY 2.14. *We use the same notations as in Proposition* 2.11 *and Theorem* 2.12. *Then we have $\sqrt{I'} = \sqrt{Id(P, f)}$.*

PROOF. By Lemma A.2 (5), we have $\sqrt{I'} = \sqrt{Id(\sqrt{I}, f)} = \sqrt{Id(P, f)}$. □

2.3. CRITERIA FOR REDUNDANT COMPONENT

We study how to construct a primary decomposition of the given ideal I from the decompositions of its pseudo-primary ideals and its remaining component and then we give useful criteria for finding redundant components. Let $\mathcal{Q}$ be a fixed primary decomposition of I and let $\overline{Q}_1 \cap \cdots \cap \overline{Q}_r \cap I'$ be a pseudo-primary decomposition of I. By Corollary 2.6, $\mathcal{Q}$ is divided into its disjoint subsets $\mathcal{Q}_1, \ldots, \mathcal{Q}_r$ and $\mathcal{Q}'$, and $\mathrm{Ass}(I)$ is also divided into its disjoint subsets $\mathcal{P}_1, \ldots, \mathcal{P}_r$ and $\mathcal{P}'$.

Now we choose an arbitrary primary decomposition $\widehat{\mathcal{Q}}_i$ of $\overline{Q}_i$, and $\widehat{\mathcal{Q}}'$ of I'. Then the union $\widehat{\mathcal{Q}} = \widehat{\mathcal{Q}}_1 \cup \cdots \cup \widehat{\mathcal{Q}}_r \cup \widehat{\mathcal{Q}}'$ is a general primary decomposition of I. From $\widehat{\mathcal{Q}}$ we arrive at another primary decomposition $\mathcal{Q}_{new}$ of I by eliminating *redundant* components. We note that we can use Lemma 2.15 as a very simple criterion.

LEMMA 2.15. *Let $\widehat{\mathcal{Q}}$ be a general primary decomposition. If a component Q in $\widehat{\mathcal{Q}}$ contains an intersection of some components in $\widehat{\mathcal{Q}} \setminus \{Q\}$, then Q is redundant.*

PROPOSITION 2.16. *Every $\widehat{\mathcal{Q}}_i$ is a subset of $\mathcal{Q}_{new}$.*

PROOF. By the uniqueness of the set of prime divisors, we have $\mathrm{Ass}(\overline{Q}_i) = \mathcal{P}_i$. (See Lemma A.5.) Since I' contains every $s_i^{k_i}$, each prime divisor in $\mathrm{Ass}(I')$ meets every S_i. This implies that $\mathrm{Ass}(I')$ is disjoint to every $\mathcal{P}_i$. From this, it follows directly that for each prime divisor P in $\mathcal{P}_i$, its associated primary component Q in $\widehat{\mathcal{Q}}_i$ is a unique primary component in $\widehat{\mathcal{Q}}$ which associates with P. This implies that Q is left in $\mathcal{Q}_{new}$. □

From Proposition 2.16, we have to find redundant components only from a primary decomposition of the remaining ideal. By considering a pseudo-primary decomposition of I', we can show the following. (We omit the proof.)

PROPOSITION 2.17.

(1) *An isolated primary component Q' of I' appears in $\mathcal{Q}_{new}$ if and only if Q' does not contain $\overline{Q}_1 \cap \cdots \cap \overline{Q}_r$.*
(2) *A pseudo-primary component $\overline{Q'}$ of I' has a primary component appearing in $\mathcal{Q}_{new}$ if and only if $\overline{Q'}$ does not contain $\overline{Q}_1 \cap \cdots \cap \overline{Q}_r$.*

Next we consider the remaining component in extraction. Let I be a pseudo-primary ideal with radical P and let $I = Q \cap I'$ be its extraction. Moreover, let $\mathcal{Q}'$ be an arbitrary primary decomposition of I'. Then $\{Q\} \cup \mathcal{Q}'$ gives a general primary decomposition of I and, from this representation, we get a new primary decomposition $\mathcal{Q}_{new}$ of I. By considering a pseudo-primary decomposition of I', we can also show the following.

PROPOSITION 2.18.

(1) *An isolated primary component Q' of I' appears in $\mathcal{Q}_{new}$ if and only if Q' does not contain Q.*
(2) *A pseudo-primary component $\overline{Q'}$ of I' has a primary component which appears in $\mathcal{Q}_{new}$ if and only if $\overline{Q'}$ does not contain Q.*

Finally we give another criterion for eliminating redundant components in a general setting. Here we consider an arbitrary ideal I of R with a general primary decomposition $\widehat{\mathcal{Q}}$. We provide necessary definitions and notations.

DEFINITION 2.19. *For a prime ideal P, we set $\mathrm{Ass}(I,P) = \{P' \in \mathrm{Ass}(I) \mid P' \subset P, P' \neq P\}$ and for a positive integer s, we set $\mathrm{Ass}(I,s) = \{P' \in \mathrm{Ass}(I) \mid \dim(P') > s\}$. For a subset $\mathcal{U}$ of $\mathrm{Ass}(I)$, we denote by $I_{\mathcal{U}}$ the ideal $\cap_{Q \in \hat{\mathcal{Q}}, \sqrt{Q} \subset P, P \in \mathcal{U}} Q$. For simplicity, we denote $I_{\mathrm{Ass}(I,P)}$ and $I_{\mathrm{Ass}(I,s)}$ by I_P and I_s, respectively.*

LEMMA 2.20. *Let $\mathcal{U}$ be a subset of $\mathrm{Ass}(I)$. Then $I_{\mathcal{U}}$ is independent of the particular general decomposition of I.*

PROOF. Let $M = R \setminus \cup_{P \in \mathcal{U}} P$. By the property of prime ideals, M is a multiplicatively closed set. By Lemma A.4, $IR_M \cap R = \cap_{Q \in \hat{\mathcal{Q}}, \sqrt{Q} \cap M = \emptyset} Q$. To prove the lemma, it suffices to show $I_{\mathcal{U}} = IR_M \cap R$, because $IR_M \cap R$ is determined uniquely by I and $\mathcal{U}$.

Now we use the property that if an ideal is contained in a finite union of prime ideals, it is contained in one of them (see Proposition 1.11 in Atiyah & MacDonald, 1969). Then for each Q in $\widehat{\mathcal{Q}}$, if $\sqrt{Q} \cap M = \emptyset$, then $\sqrt{Q} \subset \cup_{P \in \mathcal{U}} P$ and so $\sqrt{Q}$ is contained in some P belonging to $\mathcal{U}$. □

Ideals I_P and I_s are independent of the particular general primary decomposition of I.

PROPOSITION 2.21. *Let J be an ideal containing I and $\mathcal{U} = \{P \in \mathrm{Ass}(I) \mid P \subset P'$ for some $P' \in \mathrm{Ass}(J)$, $P \notin \mathrm{Ass}(J)\}$. If $\mathrm{Ass}(I) \cap \mathrm{Ass}(J) = \emptyset$ then J contains $I_{\mathcal{U}}$.*

PROOF. Set $\mathcal{U}_0 = \{P \in \mathrm{Ass}(I) \mid P \subset P'$ for some $P' \in \mathrm{Ass}(J)\}$ and $M = R \setminus \cup_{P' \in \mathrm{Ass}(J)} P'$. As J contains I, $IR_M \cap R \subset JR_M \cap R$. By Lemma A.5 and the argument in the proof of Lemma 2.20, $IR_M \cap R = \cap_{Q' \in \hat{\mathcal{Q}}, \sqrt{Q'} \cap M = \emptyset} Q' = \cap_{Q' \in \hat{\mathcal{Q}}, \sqrt{Q'} \subset P', P' \in \mathcal{U}_0} Q' = I_{\mathcal{U}_0}$ and $JR_M \cap R = J$. If $\mathrm{Ass}(I) \cap \mathrm{Ass}(J) = \emptyset$, then $\mathcal{U}_0 = \mathcal{U}$ and so $I_{\mathcal{U}} = IR_M \cap R \subset J$. □

By Proposition 2.21 we have the following criterion.

COROLLARY 2.22. *Let Q be a primary ideal of dimension d with its associated prime P. Suppose that Q belongs to a general primary decomposition $\widehat{\mathcal{Q}}$ of I such that Q is the unique component associated with P. Then the following are equivalent.*

(1) *Q appears in the primary decomposition $\mathcal{Q}_{new}$ obtained from $\widehat{\mathcal{Q}}$.*
(2) *Q does not contain I_P.*
(3) *Q does not contain I_d.*

REMARK 2.1. *Let $\{Q_1, \ldots, Q_r\}$ be a general primary decomposition of I such that $\sqrt{Q_i} \neq \sqrt{Q_j}$ for $i \neq j$. Then, the criterion derived from Corollary 2.22 is also valid for an intersection J of some primary ideals Q_i of dimension d as follows.*

Let $J = Q_{i_1} \cap \cdots \cap Q_{i_t}$, where $\dim(Q_{i_j}) = d$ for $j = 1, \ldots, t$. Then, there is an irredundant component among $\{Q_{i_1}, \ldots, Q_{i_t}\}$ if and only if J does not contain I_d.

This criterion works very well if we apply it to methods based on Gianni et al.'s approach. Because in the decomposition $I = (IR_f \cap R) \cap Id(I, f^k)$ used in those methods, every prime divisor of $IR_f \cap R$ has the same dimension.

3. The Primary Decomposition Procedure

3.1. OUTLINE OF THE PROCEDURE

Now we give an outline of a new procedure of primary decomposition for a given ideal. As mentioned in Section 1, our approach requires prime decomposition of radicals of ideals. In Section 4.4, we propose one for ideals in *special form* which is used for additional prime decomposition of radicals in the whole procedure and in Section 5.1 we show our practical implementation for prime decomposition of radicals. We can choose any practical algorithm for it. For example, in our early draft (Shimoyama & Yokoyama, 1994), we used *Wang's algorithm* based on Ritt-Wu's method (Wang, 1992).

Our algorithm consists of the following sub-procedures. We fix an ideal I of R.

3.1.1 Compute a pseudo-primary decomposition $\overline{Q}_1 \cap \cdots \cap \overline{Q}_r \cap I'$ of I.

We first compute the prime decomposition of the radical $\sqrt{I}$. Then $\sqrt{I}$ is decomposed to $P_1 \cap \cdots \cap P_r$. Each P_i is given by its Gröbner basis G_i. From $G_1, \ldots, G_r$ we compute a system of separators $\{S_1, \ldots, S_r\}$. Then by the system we compute pseudo-primary components $\overline{Q}_1, \ldots, \overline{Q}_r$. If $\sqrt{I}$ is a prime ideal, the subprocedure outputs I. We call this the *trivial* pseudo-primary component.

3.1.2 For each pseudo-primary component $\overline{Q}_i$ compute its extraction $\overline{Q}_i = Q_i \cap I'_i$.

3.1.3 For each ideal, among the ideals I' and I'_i found in subprocedures 3.1.1 and 3.1.2, if it does not coincide with R, then apply the subprocedures 3.1.1,..., 3.1.4 to it.

Then we have a general primary decomposition $\widehat{\mathcal{Q}}$ of I.

3.1.4 Eliminate redundant components from $\widehat{\mathcal{Q}}$ by the criteria in Section 2.3 and combine irredundant primary components associated with the same prime ideal.

Thus we have the following procedure for primary decomposition of ideals. We will give details of the subprocedures 3.1.1 and 3.1.2 and prove the termination of the procedure in the subsequent subsections. Since in the next section we will give an efficient elimination of redundant components, we do not give details of the subprocedure 3.1.4.

PROCEDURE 3.1. ($PrimaryDecomposition(G)$)
Input: A set G of polynomials.
Output: A set $\mathcal{U}$ of pairs (Q, P) such that $\{Id(Q) | (Q, P) \in \mathcal{U}\}$ is a primary decomposition of $Id(G)$ and $Id(P)$ is the associated prime of $Id(Q)$ for every $(Q, P) \in \mathcal{U}$.
begin
  $\mathcal{U} \leftarrow \{\}$
  $\mathcal{PL} \leftarrow$ *a set of Gröbner bases of the prime components of* $\sqrt{Id(G)}$
  $(\mathcal{QL}, G') \leftarrow PseudoPrimaryDecomposition(G, \mathcal{PL})$
  for each $(\overline{Q}, P)$ *in* $\mathcal{QL}$ *do*
    $(Q, G'') \leftarrow Extraction(\overline{Q}, P)$
    $\mathcal{U} \leftarrow \mathcal{U} \cup \{(Q, P)\}$
    if $Id(G'') \neq R$ *then* $\mathcal{U} \leftarrow \mathcal{U} \cup PrimaryDecomposition(G'')$
  if $Id(G') \neq R$ *then* $\mathcal{U} \leftarrow \mathcal{U} \cup PrimaryDecomposition(G')$
  $\mathcal{U} \leftarrow$ *set of shortest irredundant components of* $Id(G)$ *in* $\mathcal{U}$.
  return $\mathcal{U}$
end

3.2. PSEUDO-PRIMARY DECOMPOSITION

Let I be an ideal of R with a generating set G and let $P_1, \ldots, P_r$ be all isolated prime divisors of I. Moreover, let G_i be a Gröbner basis of P_i for each i. If $r = 1$, then the ideal I is a pseudo-primary ideal (trivial pseudo-primary component) and we can stop. Otherwise we compute a pseudo-primary decomposition of I by the procedures below.

3.2.1 Compute a system $\{S_1, \ldots, S_r\}$ of separators of I.

Since each P_i is a minimal element in $\mathrm{Ass}(I)$, $G_i \setminus P_j \neq \emptyset$ for $i \neq j$. From this fact, we can provide several examples for a finite set S_i as follows;

(a) a set with $r-1$ elements $\{t_1, \ldots, t_{i-1}, t_{i+1}, \ldots, t_r\}$,
(b) a singleton set $\{\prod_{j\neq i}^{r} t_j\}$,

where t_j is an element chosen from $G_j \setminus P_i$. Since G_j is a Gröbner basis of P_j, the membership of each element in G_j to P_i can be tested easily by its normal form with respect to G_i. By using the property of prime ideals, we can show that each S_i obtained by (a) or (b) becomes a separator of I with respect to P_i.

3.2.2 For each i, we compute the localization $IR_{S_i} \cap R$.

We compute $IR_{S_i} \cap R$ by $Id(G \cup \{s_{i,1}y_1 - 1, \ldots, s_{i,t}y_t - 1\}) \cap R$, where $S_i = \{s_{i,1}, \ldots, s_{i,t}\}$, and $y_1, \ldots, y_t$ are new indeterminates (see Lemma A.7). We denote by $\overline{Q}_i$ the localization $IR_{S_i} \cap R$. In the actual implementation, the efficiency of the algorithm depends on the choice of S_i. We will discuss this in Section 5.2.

3.2.3 Compute an integer k_i such that $(I : s_i^{k_i}) = \overline{Q}_i$ for each i, where $s_i = \prod_{t\in S_i} t$. From Theorem 2.7, we have $I = \overline{Q}_1 \cap \cdots \cap \overline{Q}_r \cap Id(I, s_1^{k_1}, \ldots, s_r^{k_r})$.

To find an integer k_i above, we use the following lemma as a criterion.

LEMMA 3.1. *Let J be an ideal and let s be an element of R. For a positive integer k, $(J : s^k) = JR_s \cap R$ if and only if hs^k belongs to J for every element h in a generating set of $JR_s \cap R$.*

By testing the criterion above for each positive integer in increasing order, we shall find the smallest k such that $(I : s_i^k) = IR_{S_i} \cap R$. For details, see Section 5.2.

PROCEDURE 3.2. ($PseudoPrimaryDecomposition(G, \mathcal{PL})$)
Input: A set G of polynomials and the set $\mathcal{PL}$ of Gröbner bases of all prime components of the radical of $Id(G)$.
Output: A pair $(\mathcal{QL}, G')$ such that $\mathcal{QL}$ is a set of pairs of pseudo-primary components and their radicals, and G' is a generating set of the remaining component of $Id(G)$.
begin
  if $\mathcal{PL} = \{P\}$ then return $(\{(G, P)\}, \{1\})$
  $\mathcal{QL} \leftarrow \{\}$, $G' \leftarrow G$
  for each P in $\mathcal{PL}$ do
    $S \leftarrow$ a separator with respect to P
    $\overline{Q} \leftarrow$ a generating set of the localization $Id(G)_S \cap R$
    $\mathcal{QL} \leftarrow \mathcal{QL} \cup \{(\overline{Q}, P)\}$
    $s \leftarrow$ the product of all elements in S
    $k \leftarrow$ an integer such that $(I : s^k) = \overline{Q}$
    $G' \leftarrow G' \cup \{s^k\}$
  return $(\mathcal{QL}, G')$
end

3.3. EXTRACTION ON A PSEUDO-PRIMARY IDEAL

Let I be a pseudo-primary ideal which does not coincide with R. Suppose that its radical P is given by a Gröbner basis with respect to an admissible order $>$.

3.3.1 Find a *maximally independent set* U modulo P.

We compute a maximal strongly independent set U modulo P (see Definition A.9). By Theorem 1 in Kalkbrener & Sturmfels (1993) (Lemma A.12), U becomes a maximally independent set modulo P. Then choose a block order $>'$ which satisfies $X \setminus U \gg U$. (U is also a maximal strongly independent set modulo P with respect to the order $>'$.)

3.3.2 Compute a Gröbner basis F of I with respect to $>'$ and compute the extractor f as $\mathrm{lcm}\{HC_U(g) \mid g \in F\}$, where $HC_U(g)$ is the head coefficient of a polynomial g as an element of $\mathbb{Q}(U)[X \setminus U]$ with respect to the restriction of the order $>'$ on $X \setminus U$.

3.3.3 Compute the localization $IR_f \cap R$. From Theorem 2.12, we have $Q = IR_f \cap R$, where Q is the isolated primary component of I.

3.3.4 Compute an integer k such that $(I : f^k) = Q$ by the method in the subprocedure 3.2.3. Then $I = Q \cap Id(I, f^k)$.

PROCEDURE 3.3. ($Extraction(G, P)$)
Input: A generating set G of a pseudo-primary ideal and a Gröbner basis P of $\sqrt{Id(G)}$.
Output: A generating set Q of the isolated primary component of $Id(G)$ and a generating set G' of the remaining component in the extraction.
begin
  $U \leftarrow$ *a maximally independent set modulo* $Id(P)$
  $f \leftarrow$ *the extractor associated with* $Id(G)$ *and* U
  $Q \leftarrow$ *a generating set of the localization* $Id(G)_f \cap R$
  $k \leftarrow$ *an integer such that* $(Id(G) : f^k) = Id(Q)$
  $G' \leftarrow G \cup \{f^k\}$
  return (Q, G')
end

3.4. TERMINATION OF THE PROCEDURE

The correctness of the procedure is shown by the results in Sections 3.1, 3.2 and 3.3. Here we prove the termination of this procedure.

THEOREM 3.2. *Procedure* 3.1 *terminates in finitely many steps.*

PROOF. We use an induction argument on the dimension of the ideal I given to the procedure by its generating set G. (Since R is noetherian, $\dim(I)$ is finite.) First we consider the case $\dim(I) = 0$. From Theorem 2.7 and Theorem 2.12, we can see that the remaining components in pseudo-primary decomposition and extraction become R. Thus the procedure terminates in this case.

Next we consider the case $\dim(I) > 0$ by assuming that Procedure 3.1 terminates for every ideal with dimension smaller than $\dim(I)$. If a remaining component I', i.e. either $Id(G')$ or $Id(G'')$ in the procedure, does not coincide with R, we have $\dim(I') < \dim(I)$ from Theorem 2.7 and Theorem 2.12. By the assumption of the induction, the primary decomposition procedure terminates for I'. Hence, it also terminates for I. □

4. Analysis of the Procedure and Improvements

In Procedure 3.1, we determine whether each component is irredundant or not at the final step by using several criteria proposed in Section 2.3. To improve efficiency of the procedure, we use Corollary 2.22 to eliminate each redundant component just after it is computed and avoid unnecessary pseudo-primary decompositions. In order to do this, we analyse and reformulate Procedure 3.1.

4.1. DECOMPOSITION TREE AND SEPARATING PRIME DIVISORS

First we introduce a *decomposition tree*. For the terminology of *tree*, we use the one in Aho *et al.* (1974). From now on, we call pseudo-primary decomposition and extraction *elementary operations* and fix one concrete algorithm for each.

DEFINITION 4.1. *For an ideal I, the ideals computed by an elementary operation, that is, the pseudo-primary components, the extracted primary component and the remaining component, are called* sons *of I. And I is called the* father.

For an ideal I, a decomposition tree *is a directed tree whose vertex is either a pseudo-primary component, a remaining component or a primary component appeared in Procedure 3.1. The edges are ordered pairs of a father and its son. Once we fix concrete algorithms for elementary operations, a decomposition tree is determined uniquely.*

For a decomposition tree, we can define root, ancestor, descendant, leaf *and* subtree. *Since the terminology* depth *is used both in ideal theory and graph theory, to avoid confusion we use* tree-depth*: For each vertex V in a decomposition tree of I, the* tree-depth *of V is the length of the path from I to V in the tree. Moreover, we define another depth: The* weighted tree-depth *of V is the sum of the tree-depth of V and the number of vertices V' in the path from I to V such that V' is the remaining component of its father in the pseudo-primary decomposition. We denote the weighted tree-depth of V by $wtd(V)$.*

A vertex is called a component vertex *if it is a primary ideal computed from its father by extraction, and a* non-component vertex *otherwise. For each vertex V, a component vertex which is a descendant of V is called a* component vertex under V*. All component vertices form a general primary decomposition of I and all component vertices under V form a general primary decomposition of V for a non-component vertex V. These general primary decompositions are said to be derived from the tree.*

We note that each component vertex is a leaf and each vertex contains its ancestor as ideals in R. (See an example in the Appendix.) Moreover, the subtree with root V coincides with the decomposition tree of V. Next we introduce *separating condition and reduced decomposition tree*. We fixed a decomposition tree $\mathcal{T}$ of I.

DEFINITION 4.2. *Let (V', V) be an edge such that V is a non-trivial pseudo-primary component of V' and S the separator with respect to $\sqrt{V}$ used in the pseudo-primary decomposition of V'. An ideal J of R is said to satisfy the* separating condition with respect to (V', V)*, if $\sqrt{J}$ does not contain s, where s is the product of all elements of S.*

Let V be a vertex and $\{I = V_0, V_1, \ldots, V_r = V\}$ the path from the root I to V. Then V is said to satisfy the separating condition *if V satisfies the separating condition with respect to every edge (V_i, V_{i+1}) such that V_{i+1} is a non-trivial pseudo-primary component of V_i. (If there is no such edge, V satisfies the separating condition.) In more detail, let*

$(V_{i_1}, V_{i_1+1}), \ldots, (V_{i_t}, V_{i_t+1})$ be all such edges in the path, s_j the product of all elements of the separator with respect to $\sqrt{V_{i_j+1}}$ for each j and $s = \prod_{j=1}^{t} s_i$. Then, V satisfies the separating condition if $\sqrt{V}$ does not contain s. The element s is called the tester *of V.*

The separating condition for a vertex V can be checked by a method for radical membership problem (see Becker & Weispfenning, 1993) as follows: V satisfies the separating condition if and only if $VR_s \cap R \neq R$ for its tester s.

LEMMA 4.3. *For each non-component vertex V, if V does not satisfy the separating condition, then every component vertex under V is redundant in the general primary decomposition of I derived from $\mathcal{T}$.*

PROOF. Let $\{V_0 = I, \ldots, V_r = V\}$ be the path from I to V. As V does not satisfy the separating condition, there is an edge (V_i, V_{i+1}) in the path such that V does not satisfy the separating condition with respect to (V_i, V_{i+1}). Set $\mathcal{W} = \{W \in \mathcal{T} \mid W$ is a son of V_{j-1} and $W \neq V_j$ for $1 \leq j \leq i+1\} \cup \{V_{i+1}\}$. Then $I = \cap_{W \in \mathcal{W}} W$ and the union of the general primary decompositions of all W in $\mathcal{W}$ derived from $\mathcal{T}$ forms a general primary decomposition of I. Thus, to prove the lemma it suffices to show that every component vertex under V is a redundant component of V_{i+1}. Consider the general primary decomposition $\mathcal{Q}$ of V_{i+1} derived from the tree. By Theorem 2.7, $V_i R_s \cap R = V_{i+1}$ and hence $V_{i+1} R_s \cap R = V_{i+1}$, where s is the element appearing in the condition with respect to (V_i, V_{i+1}). Since $\sqrt{V}$ contains s, we have $QR_s \cap R = R$ for every component vertex Q under V. Thus, Q is a redundant primary component of V_{i+1}. □

DEFINITION 4.4. *The* reduced decomposition tree *of I, denoted by $\mathcal{T}_{red}$, is a tree obtained from $\mathcal{T}$ by eliminating every subtree whose root does not satisfy the separating condition.*

It is easily shown that every leaf of $\mathcal{T}_{red}$ is also a component vertex. And if a component vertex V is eliminated, then its father V' is also eliminated, since $\sqrt{V} = \sqrt{V'}$.

PROPOSITION 4.5. *In $\mathcal{T}_{red}$, all component vertices have distinct associated primes.*

PROOF. Let V, V' be distinct component vertices in $\mathcal{T}_{red}$. Let U be the root of the smallest subtree containing both and let W, W' be its sons such that W is V or an ancestor of V and W' is V' or an ancestor of V'.

First consider the case where U is a pseudo-primary component. In this case we can assume $W = V$ and W' is the remaining component in the extraction. Then there is an extractor f such that f belongs to $\sqrt{W'}$ but not to $\sqrt{V}$. This implies $\sqrt{V'} \neq \sqrt{V}$.

Next consider the case where U is not a pseudo-primary component. In this case at least one of W, W' is a pseudo-primary component of U. So we can assume that W is a pseudo-primary component with a separator S. Then $\sqrt{W'}$ contains s but $\sqrt{V}$ does not, where s is the product of all elements of S. As V' contains W', we have $\sqrt{V'} \neq \sqrt{V}$. □

DEFINITION 4.6. *For each prime ideal P in* Ass(I)*, there exists a unique component vertex in $\mathcal{T}_{red}$ associated to P. We denote it by $q(P)$. For an ideal J whose radical contains some isolated prime divisor of I, we set $d(J, I) = \max\{\dim(P) \mid P \in \mathrm{Ass}_{iso}(I), P \subset \sqrt{J}\}$.*

COROLLARY 4.7. *The set $\{q(P) \mid P \in \mathrm{Ass}(I)\}$ forms a primary decomposition.*

THEOREM 4.8. *For each component vertex V in $\mathcal{T}_{red}$, $wtd(V) = 2(d(V,I) - \dim(V) + 1)$.*

PROOF. Let $m(V,I) = 2(d(V,I) - \dim(V) + 1)$. We show the theorem by an induction argument on $m(V,I)$. If $m(V,I) = 2$, then V is an isolated primary component of I and $wtd(V) = 2$. Thus we will show that the theorem holds for a pair of the ideal I and its component vertex V with $m(V,I) > 2$ by assuming that it holds for any pair of an ideal I' and its component vertex V' such that V' is not eliminated in the reduced decomposition tree of I' and $m(V',I') < m(V,I)$. (We note that if V is not eliminated in $\mathcal{T}_{red}$, then V is also not eliminated in the reduced decomposition tree of its ancestor.)

Fix an isolated prime divisor P_1 of I contained in $\sqrt{V}$ such that $\dim(P_1) = d(V,I)$. Let W be the ancestor of V with weighted tree-depth 2. By the induction, it suffices to show that $d(V,W) = d(V,I) - 1$. W is either the remaining component of a pseudo-primary component or the remaining component of I.

Consider the case where W is the remaining component of a pseudo-primary ideal $\overline{Q}$ of I. Let $\overline{Q}_1$ be the pseudo-primary component whose radical is P_1. If $\overline{Q} \neq \overline{Q}_1$, i.e. $\sqrt{\overline{Q}} \neq P_1$, then $P_1 (= \sqrt{\overline{Q}_1})$ contains the product of all elements of the separator with respect to $\overline{Q}$. As $\sqrt{V}$ contains P_1, V does not satisfy its separating condition. Thus, $\overline{Q} = \overline{Q}_1$. By Corollary 2.14, every isolated prime divisor of W is an isolated prime divisor of $\sqrt{Id(P_1, f)}$, where f is the extractor. The dimension of each isolated prime divisor of W is $\dim(P_1) - 1$ (see Lemma A.14). Hence we obtain $d(V,W) = d(V,I) - 1$.

Next consider the case where W is the remaining component of I. Now take an isolated prime divisor P' of W such that P' is contained in $\sqrt{V}$ and $\dim(P') = d(V,W)$. By Corollary 2.9, there is an isolate prime, say P_2, of I such that P' is a prime divisor of $\sqrt{Id(P_2, s_2)}$, where s_2 is the product of elements of the separator of P_2. Then P_2 is also contained in $\sqrt{V}$ and so $\dim(P_2) \leq d(V,I) = \dim(P_1)$. Since we have $\dim(P') = \dim(P_2) - 1$ by Lemma A.14, we get $d(V,W) \leq d(V,I) - 1$. On the other hand, since $P_1 \subset \sqrt{V}$ and $s_1 \in \sqrt{W} \subset \sqrt{V}$, $\sqrt{V}$ contains $\sqrt{Id(P_1, s_1)}$ and so it contains some prime divisor P'' of $\sqrt{Id(P_1, s_1)}$. Also by Lemma A.14, $\dim(P'') = \dim(P_1) - 1$. As each prime divisor of $\sqrt{Id(P_1, s_1)}$ coincides with or contains some isolated prime divisor of W, we get $d(V,W) \geq \dim(P'') = d(V,I) - 1$ and hence, $d(V,W) = d(V,I) - 1$. □

COROLLARY 4.9. *Let V, V' be component vertices in $\mathcal{T}_{red}$. If $\sqrt{V}$ is contained in $\sqrt{V'}$ properly, then $wtd(V) < wtd(V')$.*

PROOF. Let P be an isolated prime divisor of I such that P is contained in $\sqrt{V}$ and $\dim(P) = d(V,I)$. As $\sqrt{V}$ is contained in $\sqrt{V'}$, P is also contained in $\sqrt{V'}$. Thus we have $\dim(V') < \dim(V)$ and $d(V',I) \geq \dim(P) = d(V,I)$. From this, $d(V',I) - \dim(V') > d(V',I) - \dim(V) \geq d(V,I) - \dim(V)$. By Theorem 4.8, we get the corollary. □

4.2. IMPROVED PROCEDURE OF PRIMARY DECOMPOSITION

By checking the separating condition, we eliminate unnecessary non-component vertices. Thus we obtain a procedure which corresponds to the reduced decomposition tree. Moreover we incorporate an improved elimination of redundant components into it.

PROCEDURE 4.1. (*PrimaryDecomposition*(I) (IMPROVED VERSION))
Input: An ideal I of R.

Output: A primary decomposition $\mathcal{U}$ *of* I.
begin
  $H \leftarrow R$, $\mathcal{W} \leftarrow \{I\}$, $\mathcal{U} \leftarrow \emptyset$
  repeat until $H = I$ *do*
    $V \leftarrow$ *a non-component vertex of the smallest weighted tree-depth in* $\mathcal{W}$
    $\mathcal{W} \leftarrow \mathcal{W} \setminus \{V\}$
    $\mathcal{Y} \leftarrow$ *sons of elementary operation to* V
    If there is a component vertex Q *in* $\mathcal{Y}$ *such that* $H \not\subset Q$
      $\mathcal{U} \leftarrow \{Q\} \cup \mathcal{U}$, $H \leftarrow H \cap Q$
    $\mathcal{W} \leftarrow \{V \in \mathcal{Y} \mid V$ *is a non-component vertex satisfying the separating condition*$\} \cup \mathcal{W}$
  return $\mathcal{U}$
end

THEOREM 4.10. *Procedure* 4.1 *outputs a correct primary decomposition of* I.

PROOF. Since Procedure 4.1 corresponds to the reduced decomposition tree, all irredundant component vertices form a primary decomposition. Therefore, to show the correctness of the procedure, it suffices to prove that a component vertex V is irredundant if and only if V does not contain H. As H is an intersection of some primary ideals in a general primary decomposition, the *only-if* part can be shown directly.

We show the *if* part by an induction argument on the weighted tree-depth of a component vertex. If $wtd(V) = 2$, V is an isolated prime component of I and $H = R$ or an intersection of other isolated primary components of I. Therefore the claim holds. Thus we show the claim for a component vertex V by assuming that it is true for every component vertex U such that $wtd(U) < wtd(V)$. Then H is contained in the intersection of all primary components Q with $wtd(Q) < wtd(V)$. By Corollary 4.9, for each prime divisor P of I such that $P \subset \sqrt{V}$ and $P \neq \sqrt{V}$, $wtd(q(P)) < wtd(V)$. Thus $H \subset I_{\sqrt{V}}$. (For the notation, see Definition 2.19.) As V does not contain H, V also does not contain $I_{\sqrt{V}}$. By Corollary 2.22, V is irredundant. □

4.3. FAST ELIMINATION OF REDUNDANT NON-COMPONENT VERTEX

Here we show that adding one criterion we can eliminate all non-component vertices whose primary components are all redundant just after its computation. By this "fast elimination" we can give a bound on the number of required prime decompositions of radicals. We provide an additional definition and a criterion.

DEFINITION 4.11. *For each vertex* V *in* $\mathcal{T}_{red}$, *if* V *is a component vertex, then we set* $\mathcal{W}(V) = \{V\}$, *and otherwise, we set* $\mathcal{W}(V)$ *as the set of all component vertices under* V *in* $\mathcal{T}_{red}$. *We denote the intersection of all component vertices in* $\mathcal{W}(V)$ *by* $L(V)$.

For each non-component vertex V *in* $\mathcal{T}_{red}$, *we define its* complement, *denoted by* $co(V)$, *as follows. If* V *is the remaining component of its father* V' *in the pseudo-primary decomposition, then we set* $co(V) = \cap_{i=1}^{r}(U_i R_{t_i} \cap R)$, *where* $U_1, \ldots, U_r$ *are other sons of* V' *and* $t_1, \ldots, t_r$ *are their testers. Otherwise, set* $co(V) = R$. *Moreover, we define its* total

complement, *denoted by* $tco(V)$, *as* $tco(V) = \cap_{i=1}^{\ell} co(V_i)$, *where* $\{V_0 = I, \ldots, V_\ell = V\}$ *is the path from* I *to* V.

LEMMA 4.12. *Let* V *be a vertex in* $\mathcal{T}_{red}$ *and let* t *be its tester. Then* $\mathcal{W}(V)$ *is a general primary decomposition of* $VR_t \cap R$.

PROOF. We show the lemma by an induction argument on the length of a longest path from V to a leaf. Here we denote the length of a longest path from V to a leaf by $h(V)$. If V is a vertex with $h(V) = 0$, then V is a component vertex and $VR_t \cap R = V$ as $\sqrt{V}$ does not contain t. Thus the lemma holds in this case. We will show the lemma for a vertex V with $h(V) \geq 1$ by assuming that it holds for any vertex U such that $h(U) < h(V)$. Let $\mathcal{U}_0$ be the set of all sons of V in $\mathcal{T}$ and $\mathcal{U}$ that in $\mathcal{T}_{red}$. To prove the lemma, it suffices to show that for each U in $\mathcal{U}_0$, $UR_{t(U)} \cap R = UR_t \cap R$, where $t(U)$ is the tester of U. Because, from this and the assumption of the induction, we have $VR_t \cap R = \cap_{U \in \mathcal{U}_0}(UR_t \cap R) = \cap_{U \in \mathcal{U}_0}(UR_{t(U)} \cap R) = \cap_{U \in \mathcal{U}}(UR_{t(U)} \cap R) = \cap_{U \in \mathcal{U}} L(U)$.

First consider the case where V is not a pseudo-primary component. If a son U of V is the remaining component or the trivial pseudo-primary component, then its tester $t(U)$ coincides with t. If U is a non-trivial pseudo-primary component, then its tester $t(U)$ coincides with ts, where s is the product of all elements of the separator with respect to $\sqrt{U}$, and $VR_s \cap R = UR_s \cap R = U$. From this, $UR_{t(U)} \cap R = (UR_s \cap R)R_t \cap R = UR_t \cap R$.

Next consider the case where V is a pseudo-primary component of its father. Let $V = Q \cap V'$ be the extraction of the isolated primary component Q of V. Then the tester of Q and the tester of V' coincide with t. □

THEOREM 4.13. *Let* V *be a non-component vertex in* $\mathcal{T}_{red}$, t *its tester, and* H *the intersection of all primary components computed before* V *in Procedure* 4.1. *Assume* $H \neq I$. *Then every component vertex under* V *is redundant in the general decomposition of* I *if and only if* $VR_t \cap R$ *contains* $H \cap tco(V)$.

PROOF. Let $\{I = V_0, V_1, \ldots, V_r = V\}$ be the path from I to V. First we show that $\mathrm{Ass}(H \cap tco(V)) \cap \mathrm{Ass}(VR_t \cap R) = \emptyset$. By Corollary 4.9 and Lemma 4.12, we can show $\mathrm{Ass}(H) \cap \mathrm{Ass}(VR_t \cap R) = \emptyset$. Thus it suffices to show that $\mathrm{Ass}(tco(V)) \cap \mathrm{Ass}(VR_t \cap R) = \emptyset$. Assume, to the contrary, that there is a prime ideal P in $\mathrm{Ass}(tco(V)) \cap \mathrm{Ass}(VR_t \cap R)$. Then there is a vertex U such that U is a pseudo-primary component of some V_i in the path, V_{i+1} is the remaining component of V_i and P is a prime divisor of U satisfying the separating condition with respect to (V_i, U), that is, P does not contain the product s of all elements of the separator of $\sqrt{U}$. Since P is also a prime divisor of V which contains V_{i+1}, P contains s. This is a contradiction.

Now we show the theorem. Since $H \cap tco(V)$ is an intersection of some primary ideals in a general primary decomposition of I, if $VR_t \cap R$ contains $H \cap tco(V)$, then $q(P)$ is redundant for each P in $\mathrm{Ass}(VR_t \cap R)$. This shows the *if* part.

We show the *only-if* part by Proposition 2.21. Assume that $\mathrm{Ass}(VR_t \cap R) \cap \mathrm{Ass}(I) = \emptyset$. Let $\mathcal{U} = \{P \in \mathrm{Ass}(I) \mid P \notin \mathrm{Ass}(VR_t \cap R), P \subset P' \text{ for some } P' \in \mathrm{Ass}(VR_t \cap R)\}$. Then $I_{\mathcal{U}} = \cap_{P' \in \mathcal{U}} q(P')$. By Proposition 2.21, $VR_t \cap R$ contains $I_{\mathcal{U}}$. On the other hand, it can be shown easily that each P_i in $\mathcal{U}$ belongs to either $\mathrm{Ass}(H)$ or $\mathrm{Ass}(WR_{t'} \cap R)$ for some non-component vertex W such that W is a son of some V_i, V_{i+1} is the remaining component and t' is the tester of W. This shows that $\mathrm{Ass}(H \cap tco(V))$ contains $\mathcal{U}$ and so $I_{\mathcal{U}}$ contains $H \cap tco(V)$. Thus, $VR_t \cap R$ contains $H \cap tco(V)$. □

By removing non-component vertices V such that $\mathrm{Ass}(VR_t \cap R) \cap \mathrm{Ass}(I) = \emptyset$, we can avoid unnecessary prime decompositions of radicals (pseudo-primary decompositions) and then we obtain a bound on the number of necessary prime decompositions of radicals.

THEOREM 4.14. *The number of prime decompositions of radicals executed in Procedure* 4.1 *with the criterion given in Theorem* 4.13 *is bounded by* $1 + e \times d$, *where* $e = |\mathrm{Ass}(I) \setminus \mathrm{Ass}_{iso}(I)|$ *and* $d = \max\{d(P, I) - \dim(P) \mid P \in \mathrm{Ass}(I)\}$.

PROOF. Let N be the number of prime decompositions of radicals in the procedure. For each P in $\mathrm{Ass}(I)$, let $n(P)$ be the number of pseudo-primary decompositions executed in the path from I to $q(P)$. By Theorem 4.8, $n(P)$ is bounded by $d(q(P), I) - \dim(P) + 1 = d(P, I) - \dim(P) + 1$. We note that every $n(P)$ counts the pseudo-primary decomposition of I in common. Since pseudo-primary decompositions are executed only for non-component vertices V such that there is an irredundant component vertex under V, we can show that N is bounded by $1 + \sum_{P \in \mathrm{Ass}(I) \setminus \mathrm{Ass}_{iso}(I)} (n(P) - 1)$. As $n(P) - 1 = d(P, I) - \dim(P) \leq d$ for all P in $\mathrm{Ass}(I)$ we have $N \leq 1 + e \times d$. □

4.4. SPECIAL PRIME DECOMPOSITION OF RADICALS

Here we present a *special* algorithm for prime decomposition of radicals of remaining components. Let V be a non-component vertex which is the remaining component of its father in its elementary operation. By Corollary 2.9 and 2.14, the prime decomposition of its radical $\sqrt{V}$ is reduced to those of ideals, each of which is generated by one prime ideal and one element. Since this reduction gives an *intermediate* decomposition, it can improve the efficiency (see Section 6). However, we do not obtain a bound on the number of prime decomposition of radicals of such ideals.

Now we consider an ideal $Id(P_0, s)$, where P_0 is a prime ideal and s is an element of R not belonging to P. We can assume that $Id(P_0, s) \neq R$. Then all isolated prime divisors of $Id(P_0, s)$ have the same dimension $\dim(P_0) - 1$ (see Lemma A.14). Making use of this special property of $Id(P_0, s)$, we can give a special method based on Gianni *et al.*'s approach. First we provide the following in a slightly more general setting.

LEMMA 4.15. *Let* I *be an ideal of* R *and* P *its isolated prime divisor which has the largest dimension among all isolated prime divisors of* I. *Then for any admissible order* $<$ *every maximal strongly independent set* U *modulo* P *is also a maximal strongly independent set modulo* I.

PROOF. Let U be a maximal strongly independent set modulo P with respect to $<$. Then $HT(P) \cap T(U) = \emptyset$ and $|U| = \dim(P)$ by Theorem 1 in Kalkbrener & Sturmfels (1993) (Lemma A.12). Since P contains I, $HT(P)$ contains $HT(I)$ and so $HT(I) \cap T(U) = \emptyset$. Thus U is a strongly independent set modulo I. (By $HT(I)$ we denote the set of head terms of all non-zero elements of I with respect to $<$ and by $T(U)$ we denote the set of all terms in U.) Now we show that U is a maximal strongly independent set modulo I. Assume, to the contrary, that there is a maximal strongly independent set V modulo I which contains U properly. By Lemma 1.7 in Kredel & Weispfenning (1988) (Lemma A.13), there is an isolated prime P' such that V is a maximal strongly independent set modulo P'. As $\dim(P) = |U| < |V| = \dim(P')$, this contradicts the choice of P. □

By Lemma 4.15, if we already know that the given ideal I has its dimension at most d, we can compute all isolated prime divisor of I with dimension d by prime decomposition of I over $\mathbb{Q}_U = \mathbb{Q}(U)[X \setminus U]$ for all maximal strongly independent sets U of cardinality d. To avoid unnecessary computation of prime decomposition of I over $\mathbb{Q}_U$, we use "remaining" ideals. Now we present our special algorithm.

PROCEDURE 4.2. ($SpecialPrimeDecomposition(d, I)$)
Input: A positive integer d and an ideal I such that $\dim(I) \leq d$.
Output: A set $\mathcal{PL}$ of isolated prime divisor of I with dimension d.
begin
  $\mathcal{PL} \leftarrow \{\}$, $J \leftarrow I$
  $\mathcal{U} \leftarrow$ *the set of all maximal strongly independent sets modulo I with d elements*
  for all U in $\mathcal{U}$ do
    If U is not a strongly independent set modulo J then continue
    $\mathcal{P}^* \leftarrow$ *the set of all prime divisors of I computed in $\mathbb{Q}_U$*
    $\mathcal{PL} \leftarrow \{P^* \cap R \mid P^* \in \mathcal{P}^*\} \cap \mathcal{PL}$
    $H \leftarrow$ *a Gröbner basis of I with respect to a block order $U \ll X \setminus U$*
    $f \leftarrow lcm\{HC_U(g) \mid g \in H\}$, $J \leftarrow Id(J, f)$
  return $\mathcal{PL}$
end

The set of all prime divisors of I over $\mathbb{Q}_U$ can be computed by existing algorithms for prime/primary decomposition of 0-dimensional ideals, and also ideal contraction can be done by existing algorithms (see Becker & Weispfenning, 1993).

Since every isolated prime divisor of $Id(P_0, s)$ is of dimension $\dim(P_0) - 1$, by applying Procedure 4.2, we obtain all its isolated prime divisors and the prime decomposition $\sqrt{(Id(P_0, s))} = \cap_{P \in \mathcal{PL}} P$. As every prime divisor has the same dimension $\dim(P_0) - 1$, this decomposition is irredundant.

Now we show the correctness of the procedure. Here we fix an ideal I with dimension d and an order $<$. (If $\dim(I) < d$, Procedure 4.2 outputs the empty set.) Let $U_1, \ldots, U_m$ be all maximal strongly independent set modulo I with respect to $<$ appearing in this order in the procedure. The following lemma proves the correctness of the procedure.

LEMMA 4.16.

(1) *At the step for U_i, if U_i is a strongly independent set modulo J, then there is an isolated prime divisor P of I with dimension d such that P appears at this step for the first time.*
(2) *For an isolated prime divisor P of I with dimension d, if non of $U_1, \ldots, U_i$ but U_{i+1} is a maximal strongly independent set modulo P then P appears at the step for U_{i+1}.*

PROOF.

(1) As $\dim(J) \leq \dim(I) = d$, if U is a strongly independent set modulo J with d elements, then U is maximal. By Lemma A.13, there is a prime divisor P of J such that U is a maximal strongly independent set modulo P. This implies that $\dim(P) = d$. As P contains J and so I, P contains $\sqrt{I} = \cap_{P' \in \mathrm{Ass}_{iso}(I)} P'$. Since $\dim(P') \leq d = \dim(P)$

for every P' in $\mathrm{Ass}_{iso}(I)$, we have $P = P'$ for some P' in $\mathrm{Ass}_{iso}(I)$. Now we show that P does not appear at previous steps. Suppose the contrary. Then we have added some element f outside P to J. This implies that P cannot be a prime divisor of J, a contradiction.

(2) Let J be the ideal appearing at the step for U_{i+1}. We can show that P is an isolated prime divisor of J. Moreover we have $\dim(J) = \dim(I)$ which implies that P is an isolated prime divisor which has the largest dimension in $\mathrm{Ass}_{iso}(J)$. By Lemma 4.15, U_{i+1} is a maximal strongly independent set modulo J. Thus P is computed at this step. □

REMARK 4.1. *The following argument shows a certain* efficiency *of Procedure* 4.2 *for* I.

(1) *The number of prime decompositions of* 0*-dimensional ideals over rational function fields is bounded by the number of isolated prime divisors of* I.
(2) *Prime decomposition of* 0*-dimensional ideals over rational function fields is done only for* I *with some different rational function fields.*
(3) Remaining ideals J *are used for checking the strong independency of variable sets. Their Gröbner bases with respect to any order can be used for the check.*

5. Practical Implementation

Here we report on practical realizations of all the subprocedures. As a general remark, we mention that the most efficient order, *reverse lexicographical order* or *block order*, is chosen for each Gröbner basis computation.

5.1. PRIME DECOMPOSITION OF RADICALS

We outline the procedure of prime decomposition of radicals in our implementation. First we recall the following useful decompositions. The decomposition (D) can be shown by considering its varieties and the decomposition (E) follows from Lemmas A.2 and A.3.

$$\sqrt{Id(I, fg)} = \sqrt{Id(I, f)} \cap \sqrt{Id(I, g)} \tag{D}$$

$$\sqrt{I} = \sqrt{(IR_f \cap R)} \cap \sqrt{Id(I, f)}. \tag{E}$$

As mentioned before, we implemented two kinds of procedures for prime decomposition of radicals, a general one applicable to arbitrary ideals and a special one applicable to ideals generated by one prime ideal and one element.

Implementation of the General Procedure

We implemented the following procedure obtained by modifying Algorithm PRIMDEC in Becker & Weispfenning (1993) for prime decomposition. Let I be an arbitrary ideal of R. We denote $\mathbb{Q}(U)[X \setminus U]$ by $\mathbb{Q}_U$.

(1) By using decompositions (D) and (E) repeatedly, we compute ideals J_i such that
(i) $\sqrt{I} = \sqrt{J_1} \cap \cdots \cap \sqrt{J_s}$,
(ii) every element of the computed Gröbner basis of J_i is irreducible in R and
(iii) $J_i\mathbb{Q}_{U_i} \cap R = J_i$ for a maximal strongly independent set U_i modulo J_i.

(2) For each J_i, we compute all its prime divisors as follows.
  (2.1) Compute the radical J_i' of the 0-dimensional ideal $J_i\mathbb{Q}_{U_i}$ in $\mathbb{Q}_{U_i}$.
  (2.2) Compute the prime decomposition $J_i' = P_{i,1}' \cap \cdots \cap P_{i,t_i}'$ of J_i'.
  (2.3) For each $P_{i,j}'$, compute its contraction $P_{i,j}$ to R. ($P_{i,j} = P_{i,j}' \cap R$.)
  Then each $P_{i,j}$ is a prime ideal of R and $\sqrt{J_i} = P_{i,1} \cap \cdots \cap P_{i,t_i}$.
(3) Eliminate redundant components among $P_{i,j}$'s. (An ideal $P_{i,j}$ is redundant if and only if it contains other $P_{i',j'}$ properly.)

In our experiments, the decompositions (D) and (E) work very well to give an intermediate decomposition of the ideal so that the total efficiency seems to improve considerably. Since these decompositions are applicable only for radical ideals, for primary decomposition we cannot incorporate them into the original algorithm.

Implementation of the Special Procedure

To make Procedure 4.2 more practical, we incorporate the decomposition (D) into it as *pre-procedure*. Let I be an ideal generated by a prime ideal and one element.

Pre-Procedure: By applying the decomposition (D) to the given ideal I, we compute ideals I_i, $i = 1, \ldots, r$, such that $\sqrt{I} = \sqrt{I_1} \cap \cdots \cap \sqrt{I_s}$ and every element of the computed Gröbner basis of I_i is irreducible in R for each i.

Here we call each I_i a *pre-component* of $\sqrt{I}$. Then gathering isolated prime divisors of dimension $\dim(I)$ of all pre-components I_i's, we obtain the prime decomposition of $\sqrt{I}$. If I_i has an isolated prime divisor P of dimension $\dim(I)$, P has the largest dimension among all isolated prime divisors of I_i and Lemma 4.15 holds for P and I_i. Thus we can apply the following modification of Procedure 4.2. Moreover, since pre-components tend to be prime for many cases, we added test of the primality of those ideals as a *quick-test*. This test for each pre-component J can be done by choosing one maximally independent set U modulo J and testing if $J\mathbb{Q}_U$ is prime and $J = J\mathbb{Q}_U \cap R$.

PROCEDURE 5.1. (*PrimeDecomposition*(I) (SPECIAL VERSION))
Input: An ideal I such that every isolated prime divisor has the same dimension.
Output: A set $\mathcal{PL}$ of all prime divisors of $\sqrt{I}$.
begin
  $\mathcal{PL} \leftarrow \{\}$, $d \leftarrow \dim(I)$
  $\mathcal{I} \leftarrow$ *the set of all pre-components of I obtained by Pre-Procedure.*
  for each J in $\mathcal{I}$
    if $\dim(J) \neq d$ *then continue*
    if J is prime then $\mathcal{PL} \leftarrow \{J\} \cup \mathcal{PL}$
    else $\mathcal{PL} \leftarrow SpecialPrimeDecomposition(d, J) \cup \mathcal{PL}$
  return $\mathcal{PL}$
end

REMARK 5.1. *In our experiment, for many cases the pre-procedure decomposes the given ideal to its prime components.* 147 *ideals are computed by the pre-procedure from all examples in Section* 6. *Among them* 142 *ideals* (96.6%) *are already prime. Thus, for many examples the procedure terminates at the first prime check.*

5.2. MULTIPLICATIVELY CLOSED SETS AND REMAINING COMPONENTS

Pseudo-primary decomposition and extraction are also main parts of the procedure. In implementation the efficiency of the procedure depends on the choice of separators and extractors. We provide the following useful lemma. The first statement follows from Lemma A.3 (4) and the second one can be shown by Lemma 8.1 in Gianni *et al.* (1988).

LEMMA 5.1. *Let I be an ideal and s an element.*

(1) $IR_s \cap R = IR_{\{s_1,\ldots,s_m\}} \cap R = IR_{\{s_1\times\cdots\times s_m\}} \cap R$, *where* $s_1, \ldots, s_m$ *are all distinct irreducible factors of* s *in* R.
(2) *Suppose that* $(I : s^k) = IR_s \cap R$ *and* $I = (I : s^k) \cap Id(I, s^k)$. *For a factor* h *of* s^k, *if* $(I : h) = (I : s^k)$, *then* $I = (I : h) \cap Id(I, h)$ *and* $(I : h) = IR_h \cap R$.

Multiplicatively Closed Set

In the subprocedure 3.2.1 we proposed the following candidates for S_i,

(a) a set with $r - 1$ elements $\{t_1, \ldots, t_{i-1}, t_{i+1}, \ldots, t_r\}$,
(b) a singleton set $\{\prod_{j\neq i}^{r} t_j\}$,

where t_j is an element of $G_j \setminus P_i$. The choice of such t_j and the choice of the strategy (a) or (b) are very crucial for efficient computation of the localization. By using (b), we can reduce the number of additional variables to one, but we have to deal with a polynomial having large degree. Thus, it is difficult to decide which candidate is superior in theory. In actual computation, from our experiment on several examples, we conclude that a procedure with (b) is much more efficient than that with (a).

Furthermore, we can improve a procedure with (b). By Lemma 5.1, in order to compute the localization using (b), the element $s_i = \prod_{j\neq i}^{r} t_j$ can be replaced with the *maximal square-free factor* of s_i, i.e. the product of all distinct irreducible factors of s_i in R. Thus, when s_i is (square-free) factorized as $\prod m_\alpha^{e_\alpha}$, we had better use the following separator

(c) $\{\prod m_\alpha\}$,

since the degree of the polynomial in (c) may be smaller than that of s_i. Thus, in the implementation, we use a procedure with (c). We choose each t_j from $G_j \setminus P_i$ as follows.

(1) Choose a monomial from $G_j \setminus P_i$ if exists.
(2) Otherwise, choose an element from $G_j \setminus P_i$ so that it has the smallest order with respect to the order used for Gröbner basis computation.

Although we do not have any theoretical analysis on the choice, we chose the strategy (2) from the observations in several examples. Monomial is suited for the choice (c).

As for extraction (the subprocedure 3.3.2), we can use the same arguments as above. Thus, for an extractor f, we get the same localization by the maximal square-free factor h of f. By this replacement, the efficiency of the procedure will be improved.

Remaining Components

Our experiment shows that the growth of generators of the remaining components makes the total efficiency worse. More precisely, for non-component vertices, according to their tree-depths their decompositions become harder due to the growth of their generating sets. Therefore it is better to keep their generating sets as small as possible. To do this we use Lemma 5.1 (2).

Consider extraction. Let Q be the isolated primary component of a pseudo-primary ideal I. The remaining component I' is given by $Id(I, {f_0}^k)$, where f_0 is the maximal square free factor of the extractor f of I and k is an integer which satisfies $(I : {f_0}^k) = Q$. In actual computation ${f_0}^k$ tends to become very large. Thus, if there is a proper factor h of ${f_0}^k$ such that $(I : h) = (I : {f_0}^k)$, it is better to replace ${f_0}^k$ by h. Because, in this case, $Id(I, h)$ also satisfies Theorem 2.12 and $\sqrt{Id(I,h)} = \sqrt{Id(\sqrt{Q}, h)}$. To find k, we might use Lemma A.7. However, by the method in A.7, we have to compute "reverse" expressions of elements of a Gröbner basis of an ideal as linear sums of its given generator. In our experiment, the proposed method in the subprocedure 3.2.3 seems much more efficient than that in Lemma A.7.

Next we decompose f_0 into its factors $f_1, \ldots, f_t$. By decreasing lexicographical orders, from the integer vector $(k, \ldots, k)$ we obtain the "minimal" integer vector $(e_1, \ldots, e_t)$ which satisfies $(I : f_1^{e_1} \cdots f_t^{e_t}) = Q$. Here, we allow zero for each e_i. This test can be done by the same procedure as in the subprocedure 3.2.3 based on Lemma 3.1.

For pseudo-primary decomposition, we also use the same replacement. Let $\overline{Q}_1, \ldots, \overline{Q}_r$ be pseudo-primary components of I with respect to a system of separators $\{S_1, \ldots, S_r\}$ and let I' be the remaining component of I in pseudo-primary decomposition. I' is computed by $Id(I, s_1^{k_1}, \ldots, s_r^{k_r})$, where s_i is the product of all elements of S_i and k_i is a positive integer derived in Theorem 2.7. Then we can replace I' by $Id(I, h_1, \ldots, h_r)$, where each h_i is a factor of $s_i^{k_i}$ such that $(I : h_i) = \overline{Q}_i$. Since $IR_{h_i} \cap R = (I : h_i)$, we can use the same argument as in the proof of Theorem 2.7 to show that $Id(I, h_1, \ldots, h_r)$ becomes another remaining component which satisfies Theorem 2.7. And $\sqrt{Id(I, h_1, \ldots, h_r)} = \cap_{i=1}^{r} \sqrt{Id(P_i, h_i)}$, where $P_i = \sqrt{\overline{Q}_i}$ for each i.

5.3. OTHER EFFORTS

Quick Redundancy Check for Remaining Component

In Theorem 4.13 we proposed a criterion for eliminating *redundant* non-component vertices. However, in many examples, for each non-component vertex V such that V is the remaining component of its father V' in its elementary operation, the following *quick test* works very well for that purpose. We remark that the test can be done without computing a Gröbner basis of V which is necessary to test the criterion in Theorem 4.13.

Quick Test: Let V be a non-component vertex in the reduced decomposition tree of I such that V is the remaining component of its father V' in its elementary operation. Then, all component vertices under V are redundant if the intersection of other sons of V' coincides with V'.

Testing Separating Conditions

For testing whether a non-component vertex V satisfies its separating condition, we can use the prime decomposition of its father V'. If V is a pseudo-primary component

of V', $\sqrt{V}$ is already known and so we have only to test if $\sqrt{V}$ contains the tester of V. Otherwise, $\sqrt{V}$ can be expressed as the intersection of radicals of ideals generated by one prime ideal and one element or the radical of such an ideal by Corollary 2.9 and 2.14. Thus, to test if $\sqrt{V}$ contains the tester t of V is reduced to test if radicals of all such ideals contain t.

6. Discussion Based on Experiment

In this section we give an experimental comparison between our proposed method and an existing method based on Gianni *et al.*'s approach, and details on timings of the proposed method. Moreover, we also give a comparison with another existing system CALI on REDUCE (Gräbe, 1995a). Then, from the comparisons, we discuss the efficiency of the proposed method.

We implemented Procedure 4.1 with various improvements in Section 5. In Table 1, *c-S&Y* indicates the implementation with the criterion in Theorem 4.13 for avoiding unnecessary pseudo-primary decomposition and *S&Y* indicates the one without the criterion. We also implemented the method given by Becker & Weispfenning (1993) as the most recent and efficient one based on Gianni *et al.*'s approach. We added to it our improvement in Section 5.2 and the criterion derived from Corollary 2.22 (3) for eliminating redundant component and avoiding unnecessary primary decomposition of 0-dimensional ideals over rational function fields. (See Remark 2.1.) In Table 1, *c-B&W* indicates the implementation with the criterion derived from Corollary 2.22 (3) and *B&W* indicates the one without the criterion. These four implementations were done on the Risa/Asir system.

We studied 21 examples which are not radical and computed their primary decomposition on a UNIX workstation SUN4-20 with Super-Sparc CPU of 60MHz clock. For the sources of examples, see Appendix. The timings of the system CALI were measured by its function `primarydecomposition`, on the same machine, whose algorithm is also based on Gianni *et al.*'s approach. Table 1 shows the timings for the examples. Table 2 shows some information for the examples and details on the timings of *S&Y*. From the two tables we can extract the following which gives a certain *evidence* of the efficiency/practicality of the proposed method.

1. [*Overall comparison between two methods*] Except for three "small" examples without embedded components, the proposed method (*S&Y*) is faster than the method (*c-B&W*) based on Gianni *et al.*'s approach. The larger the example is, the faster *S&Y* tends to be over *c-B&W*.
2. [*Ratio of prime decomposition of radicals*] The ratio (7)/(*S&Y*) of the timing of prime decomposition of radicals to the whole timing seems very small. In the rather big examples I_8, Ge, Bu, the ratio is much less than 0.1. This is partly due to the reduction of the prime decomposition of the radicals of remaining components to those of the ideals generated by one prime ideal and one element and our *special* procedure for them (see Remark 5.1). So this part, we guess, is no more dominant for ideals with embedded components *in practice*.
3. [*Prime decomposition vs. primary decomposition*] The data in Table 2 (8) show the timings of prime decomposition of radicals for given ideals (see Section 5.1). So, the comparison between Table 2 (8) and Table 1 *c-B&W* shows that prime decomposition of radicals is much faster than primary decomposition in all examples.

Table 1. Comparison of Primary Decomposition (seconds) (†: quit after 3600 seconds).

	F_1	F_2	F_3	F_4	G_1	G_2	G_3	I_1	I_2	I_3
S&Y	1.03	1.27	1.00	1.06	0.74	0.82	2.31	0.42	1.36	5.11
c-S&Y	1.03	1.27	1.00	1.06	0.74	0.82	2.31	0.54	1.84	6.87
B&W	1.13	10.36	2.68	1.57	1.34	1.08	30.11	0.63	1.88	7.04
c-B&W	0.61	1.84	1.82	0.79	1.13	0.69	26.91	0.44	1.38	5.22
CALI	19.40	20.34	86.62	42.08	83.33	32.73	2858.30	21.51	1875.75	†

I_4	I_5	I_6	I_7	I_8	J	St	$C4$	Ge	Go	Bu
0.89	1.53	2.94	5.43	11.89	1.08	7.04	1.21	127.81	19.88	154.52
1.08	1.82	3.63	6.35	13.75	1.43	7.43	1.38	141.74	19.88	163.32
3.02	7.84	19.55	62.79	478.94	6.01	10.26	5.11	†	110.16	†
1.89	4.57	11.43	43.84	442.32	4.17	8.97	4.32	†	70.27	†
2117.81	†	†	†	†	82.48	36.86	33.58	†	1180.37	†

These results support our *strategy* of combining prime decomposition of radicals and effective localization.

4. [*Efficiency of special prime decomposition of radicals*] Table 2 (10) shows the timings of prime decomposition of radicals for remaining components by applying the general prime decomposition procedure to ideals generated by one prime ideal and one element. The comparison between (9) and (10) shows that Procedure 5.1 succeeds in making good use of the special structure of the input ideals.
5. [*Criterion*] Several criteria improved the efficiency of the procedures. Fast elimination of redundant components seems to work very well. However, the criterion in Theorem 4.13 succeeded in finding one redundant remaining component only for J and so it did not improve the efficiency of the procedure for those examples. The criterion in Corollary 2.22 also works very well for methods based on Gianni *et al.*'s approach.
6. [*Overall comparison with CALI*] The procedures implemented on Risa/Asir are much faster than CALI for all examples. This is partly due to the efficiency of the Gröbner bases packages and detailed practical efforts in Section 5. Thus, we can say that the implementation of the proposed method is done very successfully.

7. Concluding Remarks

Aiming at practical prime decomposition of polynomial ideals on computers, we took an approach that combines prime decomposition of radicals and extraction of primary components by localization. Our experiment shows that prime decomposition of the radical tends to be much easier than primary decomposition based on existing algorithms, and this fact supports our approach. For giving an efficient method based on this approach, we devised *effective localization* as a practical realization of localization by prime ideals and *fast elimination of redundant components* as an efficient way to deal with embedded components.

Table 2. Data for Reference (seconds).

(1) the number of variables appearing in a given ideal
(2) the dimension of a given ideal
(3) the difference of the highest dimension of isolated components and the lowest dimension of embedded components of a given ideal
(4) the number of primary components of a given ideal
(5) the number of isolated primary components of a given ideal
(6) the number of prime decompositions executed in *S&Y*
(7) the total timings of all prime decompositions executed in *S&Y*
(8) the timing of prime decomposition of the radical of a given ideal by using the general algorithm included in (7)
(9) the total timings of all prime decomposition of radicals of remaining components by using the special algorithm included in (7)
(10) the timings of all prime decomposition of the radicals of remaining components by using the general algorithm

	F_1	F_2	F_3	F_4	G_1	G_2	G_3	I_1	I_2	I_3
(1)	4	4	4	4	4	4	4	4	5	6
(2)	2	2	2	2	2	2	2	3	4	5
(3)	0	0	0	0	0	0	0	3	4	5
(4)	8	9	7	5	5	7	5	4	5	6
(5)	8	9	7	5	5	7	5	1	1	1
(6)	1	1	1	1	1	1	1	4	5	6
(7)	0.43	0.43	0.29	0.63	0.29	0.30	1.47	0.14	0.50	1.78
(8)	0.43	0.43	0.29	0.63	0.29	0.30	1.47	0.01	0.03	0.05
(9)	0	0	0	0	0	0	0	0.13	0.47	1.73
(10)	0	0	0	0	0	0	0	0.16	0.54	1.92

I_4	I_5	I_6	I_7	I_8	J	St	$C4$	Ge	Go	Bu
6	7	8	9	10	3	9	5	7	17	8
5	6	7	8	9	2	6	2	3	3	3
4	5	6	7	8	2	2	1	3	0	1
5	6	7	8	9	11	4	8	10	3	9
1	1	1	1	1	4	3	2	9	3	7
5	6	7	8	9	8	3	4	4	1	3
0.24	0.33	0.49	0.62	0.83	0.28	4.82	0.32	6.24	1.99	4.16
0.09	0.13	0.17	0.23	0.27	0.16	2.35	0.11	4.96	1.99	2.76
0.15	0.20	0.32	0.39	0.56	0.12	2.47	0.21	1.28	0	1.40
0.21	0.28	0.44	0.52	0.75	0.15	2.66	0.25	1.43	0	1.56

To obtain a practical method, we have to provide an efficient method for the first part, prime decomposition of radicals. Based on a precise analysis on the approach, we found an upper bound on the number of operations required in the whole procedure and also found that we can divide this operation into two kinds depending on the input: Only for the given ideal, we use a general method. As an attempt at practical implementation, we applied a modification of an existing method to a general method. For the remaining components, we gave a useful reduction to prime decomposition of radicals of ideals of the special form. And for ideals of the special form, we provided a special method aimed to take advantage of their special structure and gave a practical implementation.

By these efforts, we obtained very good timings in our experiments, by which the authors are convinced that the proposed method is *practical* and the part of prime

decomposition of radicals is no more dominant in the whole procedure for ideals with embedded components in practice.

As another possibility for practical implementation, since the first part is independent from the other parts, we can employ any algorithms for it. A more efficient algorithm and its implementation can improve the total efficiency of the procedure. For example, we can apply Wang's algorithm (Wang, 1992) or Gräbe's algorithm (Gräbe, 1994). Recently, Gräbe applied the same approach to primary decompositions for *modules* with factorized Gröbner basis computation (Gräbe, 1995b).

Finally we mention *effective localization*. For applications where isolated prime divisors are the main interest, we proposed a faster special version of effective localization in the Appendix. (See Shimoyama & Yokoyama, 1994.)

Acknowledgements

The authors would like to thank Dr. Dongming Wang. The presented work originates from discussions with him during his stay at FUJITSU LABORATORIES, ISIS. Also the authors would like to thank Dr. Hans-Gert Gräbe for his helpful comments, and the referees for many valuable comments and suggestions.

References

Aho, A.V., Hopcroft, J.E., Ullman, J.D. (1974). *The Design and Analysis of Computer Algorithms*. Reading, MA: Addison-Wesley.

Atiyah, M.F., MacDonald, I.G. (1969). *Introduction to Commutative Algebra*. Reading, MA: Addison-Wesley.

Alonso, M.E., Mora, T., Raimondo, M. (1990). Local decomposition algorithms. AAECC-8, Springer LNCS **508**, 208–221.

Backelin, J., Fröberg, R. (1991). How we prove that there are exactly 924 cyclic 7-roots. *Proc. of ISSAC'91*, ACM Press, 103–111.

Becker, T., Weispfenning, V. (1993). *Gröbner Bases*. New York: Springer-Verlag.

Boege, W., Gebauer, R., Kredel, H. (1986). Some examples for solving systems of algebraic equations by calculating Gröbner bases. *J. Symbolic Computation* **1**, 83–98.

Buchberger, B. (1965). Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. Doctoral Dissertation Math. Inst. University of Innsbruck, Austria.

Buchberger, B. (1985) Gröbner bases: An algorithmic method in polynomial ideal theory. In: Bose, N.K. (ed.), *Multidimensional Systems Theory*, Dordrecht: Reidel, 184–232.

Eisenbud, D., Huneke, C., Vasconcelos, W. (1992). Direct methods for primary decomposition. *Inventiones Mathematicae* **110**, 207–235.

Gianni, P., Trager, B., Zacharias, G. (1988). Gröbner bases and primary decomposition of polynomial ideals. *J. Symbolic Computation* **6**, 149–167.

Gräbe H.G. (1994). On factorized Gröbner bases. To appear in *Proc. Computer Algebra in Science and Engineering*.

Gräbe H.G. (1995a). CALI–A REDUCE package for constructive commutative algebra, Version 2.2.1. (anonymous ftp from `aix550.informatik.uni-leipzig.de`)

Gräbe H.G. (1995b). Minimal primary decomposition and factorized Gröbner bases. To appear in *Journal of Appl. Alg. in Eng. Comm. and Comp.*

Kalkbrener, M., Sturmfels, B. (1993). Initial complexes of prime ideals. To appear in *Advances in Mathematics*.

Kredel, H. (1987). Primary ideal decomposition. EUROCAL '87, Springer LNCS **378**, 270–281.

Kredel, H., Weispfenning, V. (1988). Computing dimension and independent sets for polynomial ideals. *J. Symbolic Computation* **6**, 231–247.

Lazard, D. (1985). Ideal bases and primary decomposition: case of two variables. *J. Symbolic Computation* **1**, 261–270.

Nagata, M. (1962). *Local Rings*. Tracts in Mathematics Number 13, New York: Interscience Publishers.

Noro, M., Takeshima, T. (1992). Risa/Asir—a computer algebra system. *Proc. of ISSAC'92*, ACM Press, 387–396. (anonymous ftp from `(164.71.1.131) endeavor.fujitsu.co.jp`, directory `/pub/isis/asir`)

Oaku,T. (1994). Computation of the characteristic variety and the singular locus of a system of differential equations with polynomial coefficients. *Japan J. Indust. Appl. Math.* **11**, 485–497.
Rutman, E.W. (1992). Gröbner bases and primary decomposition of modules. *J. Symbolic Computation* **14**, 483–503.
Shimoyama, T., Yokoyama, K. (1994). Localization and primary decomposition of polynomial ideals. FUJITSU ISIS Research Report, ISIS-RR-94-10E.
Wang, D. (1992). Irreducible decomposition of algebraic varieties via characteristic sets and Gröbner bases. *Computer Aided Geometric Design* **9**, 471–484.
Zariski, O., Samuel, P. (1958/60). *Commutative Algebra*, vols. I, II. Princeton, NJ, Van Nostrand. Reprint New York: Springer-Verlag, 1975/79.

Appendix A. Basic Theory of Ideals

Here we recall important notions and properties related to primary decomposition and localization. Computation of localizations can be done by Lemma A.7. Lemma A.6 shows that each isolated primary component can be extracted by the direct localization at its associated prime ideal. (Proofs of lemmas without citation are found in Becker & Weispfenning, 1993; Atiyah & MacDonald, 1969 and Nagata, 1962 or easily given.)

DEFINITION A.1. *Let $\mathcal{Q} = \{Q_1, \ldots, Q_r\}$ be a general primary decomposition of an ideal I. For some Q_i, if $I = \cap_{j \neq i} Q_i$, then the primary ideal Q_i is called a* redundant component *with respect to $\mathcal{Q}$. Otherwise, Q_i is called an* irredundant component *with respect to $\mathcal{Q}$. If all primary ideals $Q_1, \ldots, Q_r$ are irredundant components, then the general primary decomposition $\mathcal{Q}$ of I is called an* irredundant primary decomposition *of I.*

Let $\{Q_1, \ldots, Q_r\}$ be an irredundant primary decomposition of I, and let P_i be the associated prime ideal of Q_i for each i. If $P_1, \ldots, P_r$ are pairwise different, the representation is called a shortest irredundant primary decomposition.

REMARK A.1. *From a general primary decomposition of an ideal I, we can obtain a new representation by deleting one redundant component from a representation repeatedly. Then, this new representation becomes an irredundant primary decomposition of I.*

For two primary ideals Q and Q' associated with the same prime ideal P, their intersection $Q \cap Q'$ is also a primary ideal associated with P. Thus, from an irredundant primary decomposition of I, we can obtain a primary decomposition of I by combining primary components associated with the same prime ideal.

LEMMA A.2. *For operations on ideals, the following* distributive *laws hold, where I, J are ideals of R, s, t are elements of R and S, T are multiplicatively closed sets.*

(1) $(I \cap J : s) = (I : s) \cap (J : s)$ *and* $(I \cap J)R_S \cap R = (IR_S \cap R) \cap (JR_S \cap R)$.
(2) $((I : s) : t) = (I : st)$ *and* $(IR_S \cap R)R_T \cap R = IR_U \cap R$, *where* $U = \{xy \mid x \in S \text{ and } y \in T\}$.
(3) *If s is an element of I, then* $Id((I \cap J), s) = I \cap Id(J, s)$.
(4) *Let S be a finite set in R, and* $s = \prod_{t \in S} t$. *Then* $IR_S \cap R = IR_s \cap R$.
(5) $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$ *and* $\sqrt{Id(I, J)} = \sqrt{Id(\sqrt{I}, \sqrt{J})}$.

LEMMA A.3. *Let I be an ideal and f an element of R. Then there is an integer k such that $(I : f^k) = IR_f \cap R$. Moreover, in this case, we have $I = Id(I, f^k) \cap (I : f^k)$.*

LEMMA A.4. *Let Q be a primary ideal of R with associated prime P and S a multiplicatively closed set of R. If $S \cap P = \emptyset$, then $QR_S \cap R = Q$, and otherwise, $QR_S \cap R = R$.*

LEMMA A.5. *Let I be an ideal and S a multiplicatively closed set of R. Suppose that $\{Q_1, \ldots, Q_m\}$ is a primary decomposition of I such that S meets $Q_{r+1}, \ldots, Q_m$ but not $Q_1, \ldots, Q_r$. Then $IR_S \cap R = \cap_{i=1}^{r} Q_i$ and this gives a primary decomposition of $IR_S \cap R$.*

LEMMA A.6. *Let I be an ideal of R. For each isolated primary component Q of I and its associated prime P, $Q = IR_P \cap R$.*

LEMMA A.7. *Let I be an ideal of R and f an element in R. Set $J = Id(I, 1 - yf)$ an ideal of $R[y] = \mathbb{Q}[X, y]$. Then $IR_f \cap R (= (I : f^\infty))$ coincides with $J \cap R$. If $\{f_1, \ldots, f_s\}$ is a Gröbner basis of I and $\{g_1, \ldots, g_t\}$ is a Gröbner basis of $J \cap R$ with $g_i = h_i(1 - yf) + \sum_{j=1}^{s} h_{i,j} f_j$ for each i, where $h_i, h_{i,j} \in \mathbb{Q}[X, y]$, then $k = \max\{\deg_y(h_{i,j}) \mid 1 \leq i \leq t, 1 \leq j \leq s\}$ satisfies $(I : f^k) = IR_f \cap R$.*

LEMMA A.8. *Let I be an ideal of R, U any subset of X and G a Gröbner basis of I with respect to an inverse block order $<$ in X such that $U \ll X \setminus U$. Moreover, let $<'$ be the restriction of $<$ to $X \setminus U$. For each $g \in R$, we denote by $HC_U(g)$ the head coefficient of g in $\mathbb{Q}[U]$ as an element in $\mathbb{Q}(U)[X \setminus U]$ with respect to the order $<'$. Then $I\mathbb{Q}(U)[X \setminus U] \cap R = IR_f \cap R$, where $f = \mathrm{lcm}\{HC_U(g) \mid g \in G\}$.*

Next we provide the notion of *dimensions of ideals* and its related results.

DEFINITION A.9. *Let I be an ideal of R. A subset U in X is called an* independent set modulo I *if $I \cap \mathbb{Q}[U] = \{0\}$. An independent set U modulo I is called a* maximally independent set modulo I *if $I \cap \mathbb{Q}[U \cup \{x\}] \neq \{0\}$ for every variable x in $X \setminus U$.*

A subset U in X is called a strongly independent set modulo I with respect to an admissible order $<$ *if $HT(I) \cap T(U) = \emptyset$, where $T(U)$ is the set of all terms in U and $HT(I)$ is the set of head terms of all non-zero elements in I with respect to $<$. Moreover, U is called a* maximal strongly independent set modulo I with respect to $<$ *if U is a strongly independent set and $HT(I) \cap T(U \cup \{x\}) \neq \emptyset$ for every variable x in $X \setminus U$.*

We can compute a maximal strongly independent set modulo I with respect to $<$ from its Gröbner basis G with respect to $<$. Because $HT(I) \cap T(U) = \emptyset$ if and only if $HT(G) \cap T(U) = \emptyset$.

DEFINITION A.10. *Let P be a prime ideal of R. An ascending chain from P is a sequence of prime ideals of R $\{P = P_0 \subset P_1 \subset \cdots \subset P_t\}$ with $P_i \neq P_{i+1}$ for $0 \leq i \leq t$. An ascending chain of P is said to be* maximal *if there is no other chain containing it as a proper subset. The dimension of P is defined as the length of a maximal ascending chain from P and denoted by* $\dim(P)$. *(Every maximal ascending chain from P has the same length.) For an arbitrary ideal I, the* dimension of I, *denoted by* $\dim(I)$, *is defined as the maximal dimension among all isolated prime divisors of I.*

LEMMA A.11. *Let P be a prime ideal of R. The dimension* $\dim(P)$ *of P is equal to the number of elements of each maximally independent set modulo P.*

LEMMA A.12. (KALKBRENER & STURMFELS, 1993) *Let P be a prime ideal and U a maximal strongly independent set modulo I with respect to an arbitrary admissible order $<$. Then U is also a maximally independent set modulo P and $|U| = \dim(P)$.*

LEMMA A.13. (KREDEL & WEISPFENNING, 1988) *If I is a proper ideal of R and U is a maximal strongly independent set modulo I, then there exists an isolated prime divisor P of I such that U is also a maximal strongly independent set modulo P.*

LEMMA A.14. *Let P be a prime ideal and s an element of R not contained in P. If $Id(P,s) \neq R$, then $\dim(P') = \dim(P) - 1$ for every isolated prime divisor P' of $Id(P,s)$.*

Since the residue class ring R/P is a noetherian domain, Lemma A.14 can be shown by *Principal Ideal Theorem* (Theorem 29 of Chapter 4 in Zariski & Samuel, 1958).

Appendix B. Generating Sets of Examples

The following are generating sets of ideals and variable orders used for term order. We note that $F_1, \ldots, F_4$ and G_1, G_2, G_3 are taken from partial differential equations for Appell's hypergeometric functions and Horn's ones, respectively. (See Oaku, 1994.)

F_n: $\xi, \eta, x, y \quad (\xi \gg \eta \gg x \gg y)$ $\quad G_n$:ξ, η, x, y
I_n: $x_1, \ldots, x_r$ for $n = 1, 2, 3$ and $x_0, \ldots, x_r$ for $n = 4, \ldots, 8$ $\quad J$: x, y, z
St: $x_{11}, x_{12}, x_{13}, x_{21}, x_{22}, x_{23}, x_{31}, x_{32}, x_{33}$ $\quad C4$: z_1, z_2, z_3, z_4 $\quad Ge$: $l7, l6, l5, l4, l3, l2, l1$
Go: $c5, c4, c3, c2, c1, c0, b5, b4, b3, b2, b1, b0, a5, a4, a3, a2, a0$ Bu: $b1, a32, b2, b3, a, c3, c2, b$

F_1: $\{((y^2-y)x-y^3+y^2)\eta^2, (x-y)\eta\xi, (x-y^2)\eta\xi+(-y^2+y)\eta^2, (-x^2+x)\xi^2+(-yx+y)\eta\xi\}$
F_2: $\{-yx\eta\xi + (-y^2+y)\eta^2, (-x^2+x)\xi^2 - yx\eta\xi, ((-y^2+y)x - y^3 + 2y^2 - y)\eta^3, (y^2 - y)\eta^2\xi + (-y^2+y)\eta^3\}$
F_3: $\{x\eta\xi+(-y^2+y)\eta^2, (-x^2+x)\xi^2+y\eta\xi, ((y^4-2y^3+y^2)x-y^4+y^3)\eta^3, y^2\eta^2\xi+(-y^4+2y^3-y^2)\eta^3\}$
F_4: $\{-2yx\eta\xi+(-yx-y^2+y)\eta^2, x\xi^2-y\eta^2, (yx^2-(2y^2+2y)x+y^3-2y^2+y)\eta^3, (-2y^2+2y)\eta^2\xi + (yx-3y^2-y)\eta^3\}$
G_1: $\{(4y^2x^2+(4y^3+4y^2-y)x-y^2-y)\eta^2, (x+y+1)\eta\xi+(-4y^2x-4y^3-4y^2)\eta^2, (-x-2y^2-2y-1)\eta\xi + (8y^3x+8y^4+8y^3+2y^2+y)\eta^2, ((y^3+y^2)x-y^2-y)\eta^2, (y+1)\eta\xi + (-y^3-y^2)\eta^2, (x+1)\eta\xi + (-y^2-y)\eta^2, (x^2+x)\xi^2 + (-yx-y)\eta\xi\}$
G_2: $\{(y^3+y^2)x-y^2-y)\eta^2, (y+1)\eta\xi + (-y^3-y^2)\eta^2, (x+1)\eta\xi + (-y^2-y)\eta^2, (x^2+x)\xi^2 + (-yx-y)\eta\xi\}$
G_3: $\{((12y+8)x^2+(2y+2)x)\eta\xi+((-15y^2-4y)x-4y^2-y)\eta^2, -x\xi^2+((-12y-8)x+2y)\eta\xi+(15y^2+4y)\eta^2, (81y^4x^2+(-54y^3-12y^2)x-12y^3-3y^2)\eta^3, (-24yx+6y^2-6y)\eta^2\xi + (-81y^4x+81y^3+24y^2)\eta^3, (48x^2+(-30y+12)x-6y)\eta^2\xi + ((81y^3-54y^2-24y)x-21y^2-6y)\eta^3, (-96yx-18y^3+18y^2-24y)\eta^2\xi+(243y^5x-243y^4+72y^3+48y^2)\eta^3, 6y\eta^2\xi^2+((576y+384)x^2+(-81y^3-306y^2-168y+96)x+81y^2-18y)\eta^3\xi + ((-720y^2-192y)x+450y^3-60y^2-48y)\eta^4\}$
I_1: $\{{x_4}^4, x_1{x_4}^3, x_1x_2{x_4}^2, {x_2}^2{x_4}^2, {x_2}^2x_3x_4, x_1x_2x_3x_4, x_1{x_3}^2x_4, {x_3}^3x_4\}$
I_2: $\{{x_5}^5, x_1{x_5}^4, x_1x_2{x_5}^3, {x_2}^2{x_5}^3, {x_2}^2x_3{x_5}^2, x_1x_2x_3{x_5}^2, x_1{x_3}^2{x_5}^2, {x_3}^3{x_5}^2, {x_3}^3x_4x_5, x_1{x_3}^2x_4x_5, x_1x_2x_3x_4x_5, {x_2}^2x_3x_4x_5, {x_2}^2{x_4}^2x_5, x_1x_2{x_4}^2x_5, x_1{x_4}^3x_5, {x_4}^4x_5\}$

I_3: $\{x_6{}^6, x_6{}^5x_1, x_6{}^4x_2x_1, x_6{}^4x_2{}^2, x_6{}^3x_3x_2{}^2, x_6{}^3x_3x_2x_1, x_6{}^3x_3{}^2x_1, x_6{}^3x_3{}^3, x_6{}^2x_4x_3{}^3, x_6{}^2x_4x_3{}^2x_1, x_6{}^2x_4x_3x_2x_1, x_6{}^2x_4x_3x_2{}^2, x_6{}^2x_4{}^2x_2{}^2, x_6{}^2x_4{}^2x_2x_1, x_6{}^2x_4{}^3x_1, x_6{}^2x_4{}^4, x_6x_5x_4{}^4, x_6x_5x_4{}^3x_1, x_6x_5x_4{}^2x_2x_1, x_6x_5x_4{}^2x_2{}^2, x_6x_5x_4x_3x_2{}^2, x_6x_5x_4x_3x_2x_1, x_6x_5x_4x_3{}^2x_1, x_6x_5x_4x_3{}^3, x_6x_5{}^2x_3{}^3, x_6x_5{}^2x_3{}^2x_1, x_6x_5{}^2x_3x_2x_1, x_6x_5{}^2x_3x_2{}^2, x_6x_5{}^3x_2{}^2, x_6x_5{}^3x_2x_1, x_6x_5{}^4x_1, x_6x_5{}^5\}$

I_4: $\{(x_0-x_5)^5, (x_0-x_1)(x_0-x_5)^4, (x_0-x_2)(x_0-x_5)^3, (x_0-x_3)(x_0-x_5)^2, (x_0-x_4)(x_0-x_5)\}$

I_5: $\{(x_0-x_6)^6, (x_0-x_1)(x_0-x_6)^5, (x_0-x_2)(x_0-x_6)^4, (x_0-x_3)(x_0-x_6)^3, (x_0-x_4)(x_0-x_6)^2, (x_0-x_5)(x_0-x_6)\}$

I_6: $\{(x_0-x_7)^7, (x_0-x_1)(x_0-x_7)^6, (x_0-x_2)(x_0-x_7)^5, (x_0-x_3)(x_0-x_7)^4, (x_0-x_4)(x_0-x_7)^3, (x_0-x_5)(x_0-x_7)^2, (x_0-x_6)(x_0-x_7)\}$

I_7: $\{(x_0-x_8)^8, (x_0-x_8)^7(x_0-x_1), (x_0-x_8)^6(x_0-x_2), (x_0-x_8)^5(x_0-x_3), (x_0-x_8)^4(x_0-x_4), (x_0-x_8)^3(x_0-x_5), (x_0-x_8)^2(x_0-x_6), (x_0-x_8)(x_0-x_7)\}$

I_8: $\{(x_0-x_9)^9, (x_0-x_9)^8(x_0-x_1), (x_0-x_9)^7(x_0-x_2), (x_0-x_9)^6(x_0-x_3), (x_0-x_9)^5(x_0-x_4), (x_0-x_9)^4(x_0-x_5), (x_0-x_9)^3(x_0-x_6), (x_0-x_9)^2(x_0-x_7), (x_0-x_9)(x_0-x_8)\}$

J: $((z^2-z)y^2+(z^2-z)y)x, (zy^3+zy^2)x, (y^4-y^2)x, (z^2-z)yx^2, (y^3-y^2)x^2, (z^3-z^2)x^4+(2z^3-2z^2)x^3+(z^3-z^2)x^2, zy^2x^2, zyx^4+zyx^3, 2y^2x^4+6y^2x^3+6y^2x^2+(y^3+y^2)x, zx^5+(z^2+z)x^4+(2z^2-z)x^3+(z^2-z)x^2, yx^6+3yx^5+3yx^4+yx^3$

St: $\{x_{21}x_{12}-x_{22}x_{11}, x_{13}x_{22}-x_{23}x_{12}, x_{31}x_{22}-x_{32}x_{21}, x_{32}x_{23}-x_{33}x_{22}\}$

$C4$: Cyclic 4, in Backelin and Fröberg (1991)

Ge: Gerdt, Go: Gonnet, Bu: Butcher, in Boege *et al.* (1986)

Appendix C. One Example of Decomposition Tree

We show the decomposition tree of the example J corresponding to Procedure 4.1. The Ideal J has the following 11 primary components. $\{Q_1, \ldots, Q_{11}\} = \{Id(x), Id((x+1)^2, y), Id(y, z), Id((x+1)^3, y-1, z), Id(x^2, y+1), Id(x+1, y^2, z-1), Id(x-1, y, z^2), Id(x^2, y), Id((x+1)^3, y^2, z), Id(x^3, y^2, -z+1), Id(x^3, y^2, z)\}$. In the tree, each $\overline{Q_i}$ is a pseudo-primary component and each J_i is a remaining component. Vertices eliminated by criteria are marked by *elim.* (See Figure 1.)

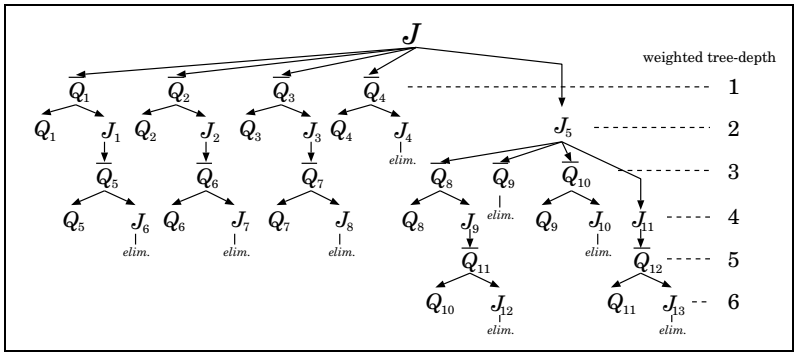

Figure 1. Decomposition tree of J.

Appendix D. Computation of Isolated Primary Components

We can modify the procedure for computation of isolated primary components. In the modified procedure, the number of computations of localization is reduced to 50%. Its correctness can be shown by combining Proposition 2.4 and Proposition 2.11. We note that if a given ideal I is already known to have no embedded components, we can get all primary components of I by using Procedure D.1 with $f = 1$.

PROCEDURE D.1. ($IsolatedPrimaryComponents(I)$)
Input: An ideal I.
Output: A set $\mathcal{U}$ *of pairs of isolated primary components of* I *and their associated primes.*
begin
  $PL \leftarrow$ *a set of Gröbner bases of all prime components of* $\sqrt{I}$, $\mathcal{U} \leftarrow \{\}$
  for each P *in* PL *do*
    $S \leftarrow$ *a separator with respect to* P
    $u \leftarrow$ *the product of all elements in* S
    $f \leftarrow$ *an element computed from* I *and a maximally independent set modulo* P
    $h \leftarrow$ *the maximal square-free factor of* $u \cdot f$
    $Q \leftarrow$ *the localization* $IR_h \cap R$
    $\mathcal{U} \leftarrow \mathcal{U} \cup \{(Q, P)\}$
  return $\mathcal{U}$
end