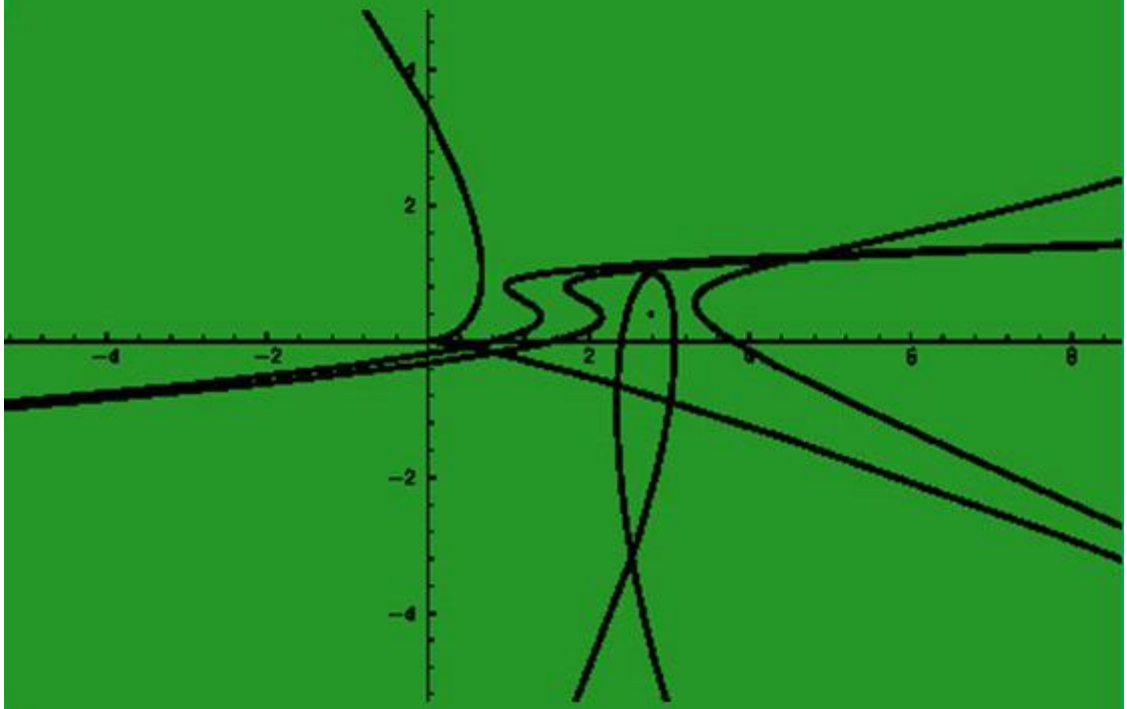
Communications of Japan Society for Symbolic and Algebraic Computation

2020
VOL.4



JSSAC

ISBN978-4-903027-36-4

Aims and Scopes:
Communications of JSSAC (Japan Society of Symbolic and Algebraic Computations) is dedicated to researchers who have a special interest in symbolic and algebraic computation. Communications of JSSAC publishes original articles dealing with every aspect of symbolic and algebraic computation.

Research Areas Include but are not limited to:
・Theoretical and algorithmic issues of symbolic and algebraic computation
・Design and implementation of symbolic and algebraic computation systems
・Applications of symbolic and algebraic computation in education, science, engineering and industry, pure mathematics, etc.

Legal Requirements:
In order to submit a manuscript, at least one of the author(s) should be a member of JSSAC in principle

Manuscript Submission:
A manuscript must be written in English.
It also should be written in Latex.
A submission must include:
(1) a Latex source file
(2) a dvi, ps or pdf file of (1)
(3) a title of the paper as well as the name(s) and affiliation(s) and mailing address(es) of the author(s)
(4) an abstract (no more than 150 words) and key words (5 or less)

For full and complete guide for authors, please refer to the following sites.

http://www.jssac.org/Editor/Style/index.html (in Japanese)
http://www.jssac.org/Editor/Communications/index-e.html (in English)

Every submitted manuscript will undergo a standard review process and the acceptance for publication by the editorial board will be based on its originality, significance of contribution and its relevance to the scope of Communications of JSSAC.

Miscellaneous:
・The copyright of a published paper is transferred to JSSAC.
・Communications of JSSAC has no page charges.

Contents

Computation of a Primary Component of an Ideal from Its Associated Prime by Effective Localization
Yuki Ishihara, Kazuhiro Yokoyama 1

Simple Signature-Based Algorithms with Correctness and Termination
Kosuke Sakata 33

Communications of JSSAC (2020)
Vol. 4, pp. 1 – 31

Computation of a Primary Component of an Ideal from Its Associated Prime by Effective Localization

Yuki Ishihara*
Graduate School of Science, Rikkyo University

Kazuhiro Yokoyama†
Department of Mathematics, Rikkyo University

(Received 23/May/2020 Accepted 26/Sep/2020)

Abstract

This is an enhanced full paper version of [Ishihara-Yokoyama, 2018] and contains detailed proofs, additional examples and new algorithms. In [Ishihara-Yokoyama, 2018], we proposed effective methods for localization of a polynomial ideal, which are called "Local Primary Algorithm (LPA)". Here, we consider the special case "localization by a prime ideal" and we introduce criteria for prime divisors and effective methods for computation of a primary component. For an ideal I and a prime ideal P, LPA computes a P-primary component of I after checking whether P is a prime divisor of I. It mainly uses *Double Ideal Quotient* (DIQ) $(I : (I : P))$ and its variants which contain useful information about localization of I. To examine its practicality, we compare it to another localization algorithm without DIQ. Based on computational experiments, we give further discussions about the practicality.

Keywords: Gröbner Basis, Primary Decomposition, Localization, Double Ideal Quotient

1 Introduction

The operation of "localization by a prime ideal" is widely known as a basic tool in commutative algebra and algebraic geometry. Here, we focus on computing a primary component from only its prime divisor and propose a new effective localization. As key notions, it uses *double ideal quotient* (DIQ) (and its variants) and *maximal independent set* (MIS).

We recall briefly the essence of [5]. Localization of ideals (as the saturation or the contraction of localized ideals) can be computed through its primary decomposition (see Remark 4), where algorithms of primary decomposition have been much studied in papers [2, 3, 7, 12]. However, in practice, the use of primary decomposition is not an efficient way since it tends to be very time-consuming. Hence, we focused on special localization (localization by a prime ideal) and compute a primary component directly, without its full primary decomposition. Then, we invented a direct method named *Local Primary Algorithm* (LPA) which computes a primary component, without its full primary decomposition. In more details, we explain some key points of LPA as follows.

*yishihara@rikkyo.ac.jp
†kazuhiro@rikkyo.ac.jp

- LPA is based on several generating tools and criteria for primary components with different procedures for two cases; isolated and embedded.
- LPA uses *double ideal quotient and its variants* as tools for generating and checking primary components.
- *Double ideal quotient* (DIQ) is $(I : (I : J))$ for ideals I and J, which already appears in [14] to check associated primes or compute equidimensional hulls, and in [2], to compute equidimensional radicals.
- There are other important properties of DIQ and its variants toward effective localization. For instance, for ideals I, J and a primary decomposition $\mathcal{Q}$ of I, a variant of DIQ $(I : (I : J)^\infty)$ coincides with $\bigcap_{Q\in\mathcal{Q},J\subset IK[X]_{\sqrt{Q}}\cap K[X]} Q$.

For practical implements we devised several efficient techniques for improving our LPA as follows (see [6, 14] for efficient computation of ideal quotient and saturation).

- ($P_G^{[m]}$-products) Use $P_G^{[m]} = (f_1^m, \ldots, f_r^m)$ for some generator $G = \{f_1, \ldots, f_r\}$ of P and the *equidimensional hull* (see Definition 10) hull$(I + P_G^{[m]})$ to compute a P-primary component, instead of using hull$(I + P^m)$ (see Lemma 54).
- (MIS-hull) Use *a maximal independent set* of P for computing hull$(\overline{Q})$ where $\overline{Q}$ is a P-hull-primary ideal (see Definition 13). Since a maximal independent set U of P is also a maximal independent set of $I + P^m$, we obtain hull$(I + P^m) = (I + P^m)K[X]_{K[U]^\times} \cap K[X]$ (see Lemma 58).
- (MIS-localization) Use a maximal independent set U of P at the first step of LPA to replace I for $IK[X]_{K[U]^\times} \cap K[X]$ (see Theorem 39).

As an enhanced full paper version of [5], this paper contains detailed proofs, additional examples and new algorithms. In particular, as additional development, we invent another localization algorithm using a well-known splitting tool of ideal instead of DIQ to compare it and the original LPAs (see Sect. 6). Furthermore, we make a new implementation on the computer algebra system Risa/Asir [11] and re-examine the performance in a number of examples in Sect. 7. As a reference, we show the timings of a full primary decomposition function `noro_pd.syci_dec` in Risa/Asir. Thanks to efficient techniques above, our experiment shows clearly the practicality of our direct localization method. From our experiments, we conclude that MIS-localization is the most efficient tool among our LPAs. However, there are some cases for which it is not efficient. Our main observation is the following;

- LPAs have strong effectiveness by its speciality.
- MIS-localization is much effective for many examples (see Table 1 and Table 2 in Sect. 7). However, its computational behavior is *unstable* (see Figures 2, 3 in Sect. 7).
- Effectiveness of the algorithms depends on ideals. At present, it is not predicable and thus it would be better to apply them in parallel.

This paper is organized as follows. Through Sect. 2 to Sect. 7, we add complete proofs and a lot of examples as an enhanced full paper version of [5]. In Sect. 2, we provide a mathematical basis for our criteria and algorithms. In Sect. 3, we introduce notions and properties of DIQ and its variants. In Sect. 4, we describe criteria for prime divisors and primary components by using DIQ and its variants. In Sect. 5, we explain LPA to compute the particular primary component

without primary decomposition, after isolated and embedded prime divisor checks. In Sect. 6, the additional section, we generalize propositions in [5] and devise a new algorithm using splitting tool and maximal independent set instead of DIQ. In Sect. 7, we tested for many examples as experiments and discuss the behavior of each algorithm. In Sect. 8, we give some concluding remarks and the future works.

2 Mathematical Basis

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

2.1 Definition of Primary Decomposition and Localization

Here we give the definition of primary decomposition, which can be found in several books [1, 3, 6, 14].

Definition 1 (Primary Decomposition)
For an ideal I of $K[X]$, a set $\mathcal{Q}$ of primary ideals is called a primary decomposition *of I if $I = \bigcap_{Q \in \mathcal{Q}} Q$. A primary decomposition $\mathcal{Q} = \{Q_1, \ldots, Q_r\}$ is irredundant if the $\sqrt{Q_i}$ are all distinct and $Q_i \not\supset \bigcap_{j \neq i} Q_j$. We assume primary decomposition is irredundant. 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. Among all prime divisors of I, minimal prime ideals are called* isolated prime divisors *of I and others are called* embedded prime divisors *of I. A primary component of I is called* isolated *if its prime divisor is isolated and* embedded *if its prime divisor is embedded. We denote by* $\mathrm{Ass}(I)$ *and* $\mathrm{Ass}_{iso}(I)$ *the set of all prime divisors of I and the set of all isolated prime divisors respectively.*

It is well-known that an isolated primary component does not depend on primary decompositions, while an embedded primary component does. From the perspective of algorithm, it tends to be more difficult to compute embedded primary components than isolated primary components.

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

Definition 2 (Localization)
Let I be an ideal of $K[X]$ and S a multiplicatively closed set in $K[X]$. We call $IK[X]_S$ the localized ideal by *S and $IK[X]_S \cap K[X]$* the contraction of the localized ideal *respectively. For simplicity, we call the latter the* localization of *I with respect to S (see Definition 2.2 in [12]). For a multiplicatively closed set $K[X] \setminus P$, where P is a prime ideal, we denote it simply by $IK[X]_P \cap K[X]$. We assume a multiplicatively closed set S always does not contain* 0.

Example 3
In $\mathbb{Q}[X] = \mathbb{Q}[x, y]$, let $P = (x)$ be a prime ideal. For $S = \mathbb{Q}[X] \setminus P$ and $I = (x^2, xy)$, the localization of I by S is $I\mathbb{Q}[X]_S \cap \mathbb{Q}[X] = (x)$. For $P = (x, y)$ and $J = (x) \cap (x + 1) \cap (x + 2, y^2)$, the localization of J by P is $J\mathbb{Q}[X]_P \cap \mathbb{Q}[X] = (x)$.

We remark a relationship between primary decomposition and localization.

Remark 4 (Localization from Primary Decomposition)
Given a primary decomposition $\mathcal{Q}$ of an ideal I, the localization of I by S is expressed as $\bigcap_{Q\in\mathcal{Q},Q\cap S=\emptyset} Q$. Moreover, it is also equal to $(I : (\bigcap_{P\in \mathrm{Ass}(I),P\cap S\neq\emptyset} P)^\infty)$. Here, we are thinking mainly about computable *multiplicatively closed set s.t. finitely generated one or the complement of a prime ideal. In these cases, we can decide efficiently whether Q and S intersect or not, by using Gröbner basis. Thus if we know all primary components or all associated primes, then we can compute localizations of I for any* computable *multiplicatively closed sets S. However, this method is not a direct method since it computes unnecessary primary components or associated primes.*

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

Definition 5 ([12], Definition 2.3)
Let Q be an ideal. We say Q is pseudo-primary *if $\sqrt{Q}$ is a prime ideal. In this case, we also say that Q is $\sqrt{Q}$-*pseudo-primary.

Example 6
Since $\sqrt{(x^2, xy)} = (x)$ is a prime ideal, it follows that (x^2, xy) is an (x)-pseudo-primary ideal. Every P-primary ideal is P-pseudo-primary.

With the notion of pseudo-primary ideal, we can define some special localization *the minimal P-pseudo-primary component* with respect to its isolated prime divisor P. It is equal to the intersection of all primary components whose radicals contain P but do not contain other isolated prime divisors.

Definition 7
Let I be an ideal and P an isolated prime divisor of I. For a set of prime divisors

$$\mathcal{P} = \{P' \in \mathrm{Ass}(I) \mid P \text{ is the unique isolated prime divisor contained in } P'\}$$

and a multiplicatively closed set $S = K[X] \setminus \bigcup_{P'\in\mathcal{P}} P'$, we call $\overline{Q} = IK[X]_S \cap K[X]$ the minimal P-pseudo-primary component *of I. This definition is consistent with one in [12]. We note that the minimal P-pseudo-primary component is determined uniquely and has the P-isolated primary component of I as component. Also, every P-pseudo-primary component of I defined in [12] contains the minimal one defined here.*

Example 8
For $I = (x) \cap (x + 1) \cap (x^2, y) \subset \mathbb{Q}[x, y]$, (x^2, xy) is the minimal (x)-pseudo-primary component of I and $(x + 1)$ is the minimal $(x + 1)$-pseudo-primary component of I.

Remark 9
Every minimal P-pseudo-primary component of I is a P-pseudo-primary ideal. Let $\overline{Q}_P$ be the minimal P-pseudo-primary component of I. Then $I = \bigcap_{P\in \mathrm{Ass}_{iso}(I)} \overline{Q}_P \cap I'$ for some I' s.t. $\mathrm{Ass}_{iso}(I') \cap \mathrm{Ass}_{iso}(I) = \emptyset$. This decomposition is called a pseudo-primary decomposition *in [12], where it is computed by separators from given $\mathrm{Ass}_{iso}(I)$. Meanwhile, we introduce another method to compute P-pseudo-primary components by using double ideal quotient in Lemma 43.*

We may regard the minimal P-pseudo-primary component as a "column localization" since it has different dimensional primary components in general. Conversely, we may consider a "row localization", that contains equidimensional primary components.

Definition 10 ([2], Sect. 1)
Let I be an ideal and $\mathcal{Q}$ a primary decomposition of I. We call $\mathrm{hull}(I) = \bigcap_{Q\in\mathcal{Q},\dim(Q)=\dim(I)} Q$ the equidimensional hull *of I. Since every primary component Q satisfying* $\dim(Q) = \dim(I)$ *is isolated,* $\mathrm{hull}(I)$ *is determined independently from choice of primary decompositions.*

Example 11
For $I = (x) \cap (x+1) \cap (x^2, y) \cap (x-1, y) \subset \mathbb{Q}[x, y]$, *it follows that* $\mathrm{hull}(I) = (x) \cap (x+1)$.

For a given I, $\mathrm{hull}(I)$ can be computed in several manners. For instance, it can be computed by Ext functors [2] or a regular sequence contained in I [14] as follows.

Proposition 12 ([2], Theorem 1.1. [14], Proposition 3.41)
Let I be an ideal and $u \subset I$ be a c-length regular sequence, where c is the codimension of I. Then $\mathrm{hull}(I) = ((u) : ((u) : I)) = \mathrm{ann}_{K[X]}(\mathrm{Ext}^c_{K[X]}(K[X]/I, K[X]))$.

Next, we introduce the notion of hull-primary ideal, which is an extension of the definition of pseudo-primary ideal. We use hull-primary ideal in Sec. 5.2.1 to devise practical techniques for LPA.

Definition 13 ([5], Definition 13)
Let I be an ideal. We say that I is hull-primary *if* $\mathrm{hull}(I)$ *is a primary ideal. For a prime ideal P, we say a hull-primary ideal I is P-*hull-primary *if* $P = \mathrm{hull}(\sqrt{I})$.

Example 14
Let $I = (x^2) \cap (x^3, y) \cap (x+1, y+1) \subset \mathbb{Q}[x, y]$. *Since* $\mathrm{hull}(I) = (x^2)$ *is (x)-primary, I is (x)-hull primary.*

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

Remark 15
Every pseudo-primary ideal is hull-primary.

Using the following lemma and a variant of *double ideal quotient*, we can compute the isolated P-primary component of I in Section 5.

Lemma 16 ([5], Lemma 15)
Let P be an isolated prime divisor of I and $\overline{Q}_P$ the minimal P-pseudo-primary component of I. Then, $\overline{Q}_P$ is a P-hull-primary and $\mathrm{hull}(\overline{Q}_P)$ *is the isolated P-primary component of I.*

Proof By Remarks 9 and 15, it follows that $\overline{Q}_P$ is P-hull-primary and $\mathrm{hull}(\overline{Q}_P)$ is the isolated P-primary component. By the definition of $\overline{Q}_P$ and Lemma 72, we obtain that $\mathrm{hull}(\overline{Q}_P)$ is the isolated P-primary component of I. ∎

Example 17
Let $I = (x) \cap (x^2, y) \cap (x^2, y+1) \subset \mathbb{Q}[x, y]$. *For* $P = (x)$, $\overline{Q}_P = (x^2, xy)$ *is the minimal P-pseudo primary component of I and* $\mathrm{hull}(\overline{Q}_P) = (x)$ *is the P-isolated primary component of I.*

2.2 Fundamental Properties of Ideal Quotient

We introduce fundamental properties of ideal quotient. The first two can be seen in several papers and books ([1], Lemma 4.4. [6], Lemma 4.1.3. [14], a remark before Proposition 3.56). The last two are direct consequences of the first two. We put a proof of Lemma 18 into Appendix.

Lemma 18 ([5], Lemma 19)
Let I and J be ideals, Q a primary ideal and $\mathcal{Q}$ a primary decomposition of I. Then,

$$(Q : J) = \begin{cases} Q & (J \not\subset \sqrt{Q}), \\ K[X] & (J \subset Q), \\ \sqrt{Q}\text{-primary ideal properly containing } Q & (J \not\subset Q, J \subset \sqrt{Q}), \end{cases} \tag{1}$$

$$(Q : J^\infty) = \begin{cases} Q & (J \not\subset \sqrt{Q}), \\ K[X] & (J \subset \sqrt{Q}), \end{cases} \tag{2}$$

$$(I : J) = \bigcap_{Q \in \mathcal{Q}, J \not\subset \sqrt{Q}} Q \cap \bigcap_{Q \in \mathcal{Q}, J \not\subset Q, J \subset \sqrt{Q}} (Q : J), \tag{3}$$

$$(I : J^\infty) = (I : \sqrt{J}^\infty) = \bigcap_{Q \in \mathcal{Q}, J \not\subset \sqrt{Q}} Q. \tag{4}$$

3 Double Ideal Quotient

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

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

For example, letting $I = (x^2) \cap (x^3, y^2) \cap (y)$, $J = (x^2)$ and $\mathcal{Q} = \{(x^2), (x^3, y^2), (y)\}$ a primary decomposition of I, it follows that $\mathcal{Q}_1(J) = \{(y)\}$, $\mathcal{Q}_2(J) = \{(x^2)\}$, and $\mathcal{Q}_3(J) = \{(x^3, y^2)\}$.

Then, our DIQ is expressed precisely by components of them. The following proposition can be proved directly from Lemma 18.

Proposition 19 ([5], Proposition 20)
Let I and J be ideals. Then,

$$\begin{aligned} (I : (I : J)) = &\bigcap_{Q \in \mathcal{Q}_2(J)} \left(Q : \left(\bigcap_{Q' \in \mathcal{Q}_1(J)} Q' \cap \bigcap_{Q' \in \mathcal{Q}_3(J)} (Q' : J) \right) \right) \\ &\cap \bigcap_{Q \in \mathcal{Q}_3(J)} \left(Q : \left(\bigcap_{Q' \in \mathcal{Q}_1(J)} Q' \cap \bigcap_{Q' \in \mathcal{Q}_3(J)} (Q' : J) \right) \right), \end{aligned} \tag{5}$$

$$\sqrt{(I : (I : J))} = \bigcap_{P \in \mathrm{Ass}(I), J \subset P} P. \tag{6}$$

Proof First, we show (5). We divide I into three parts:

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

Then,

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

Since

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

we obtain

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

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

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

The second property (6) can be proved directly from the property (5). ∎

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

Corollary 20 ([14], Corollary 3.4)
Let I be an ideal and P a prime ideal. Then, P belongs to $\mathrm{Ass}(I)$ *if and only if* $P \supset (I:(I:P))$.

Proof We note $P \supset (I:(I:P))$ if and only if $P \supset \sqrt{(I:(I:P))}$. By Proposition 19, $\sqrt{(I:(I:P))} = \bigcap_{P'\in\mathrm{Ass}(I),P\subset P'} P'$. If $P \in \mathrm{Ass}(I)$, then $\sqrt{(I:(I:P))} = \bigcap_{P'\in\mathrm{Ass}(I),P\subset P'} P' \subset P$. On the other hand, if $P \supset \sqrt{(I:(I:P))}$, then there is $P' \in \mathrm{Ass}(I)$ s.t. $P' \subset P$ and $P' \supset P$. Thus $P = P' \in \mathrm{Ass}(I)$. ∎

Example 21
Let $I = (x^2, xy)$ in $\mathbb{Q}[x,y]$. Then, $P = (x)$ is a prime divisor of I and $(I:(I:P)) = (I:(x,y)) = (x) \subset P$.

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

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

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

Proposition 23 ([5], Proposition 22)
Let $\mathcal{Q}$ be a primary decomposition of I. Then,

$$(I : (I : J)^{\infty}) = \bigcap_{Q \in \mathcal{Q}, J \subset IK[X]_{\sqrt{Q}} \cap K[X]} Q, \tag{7}$$

$$(I : (I : J^{\infty})^{\infty}) = \bigcap_{Q \in \mathcal{Q}, J \subset \sqrt{IK[X]_{\sqrt{Q}} \cap K[X]}} Q, \tag{8}$$

$$(I : (I : J^{\infty})) = \bigcap_{Q \in \mathcal{Q}_2(J)} (Q : \bigcap_{Q' \in \mathcal{Q}_1(J)} Q') \cap \bigcap_{Q \in \mathcal{Q}_3(J)} (Q : \bigcap_{Q' \in \mathcal{Q}_1(J)} Q'). \tag{9}$$

Proof Here, we give an outline of the proof. The formula (7) can be proved by combining the equation

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

by Lemma 18 and the following equivalence

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

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

for each $Q \in \mathcal{Q}$. The second formula (8) can be proved by combining the equation $(I : (I : J^{\infty})^{\infty}) = (I : (I : J^m)^{\infty}) = \bigcap_{Q \in \mathcal{Q}, J^m \subset IK[X]_{\sqrt{Q}} \cap K[X]} Q$ for a sufficiently large m from the first formula (7), and the following equivalence

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

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

for each $Q \in \mathcal{Q}$. The third formula (9) can be proved directly from Lemma 18.

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

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

then by Lemma 85, $\sqrt{Q'} \subset \sqrt{Q}$ for some $Q' \in \mathcal{Q}_1(J) \cup \mathcal{Q}_3(J)$. Since $Q' \subset \sqrt{Q'} \subset \sqrt{Q}$, we obtain $IK[X]_{\sqrt{Q}} \cap K[X] = \bigcap_{Q'' \in \mathcal{Q}, Q'' \subset \sqrt{Q}} Q'' \subset Q'$. However, since $Q' \in \mathcal{Q}_1(J) \cup \mathcal{Q}_3(J)$, we obtain $J \not\subset Q'$ and this contradicts $J \subset IK[X]_{\sqrt{Q}} \cap K[X] \subset Q'$.

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

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

Finally, we show (9). Since $(I : J^\infty) = \bigcap_{Q' \in \mathcal{Q}_1(J)} Q'$, we obtain

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

∎

Example 24
For $I = (x^2) \cap (x^3, y^2) \cap (x^4, y^3, z^2) \cap (z)$ *and* $J = (x^2)$,

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

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

Proposition 25 ([5], Proposition 23)
Let I *and* J *be ideals. Then*

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

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

Proof Let $\mathcal{Q}$ be a primary decomposition of I. By Proposition 23 (9),

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

Since $\mathcal{Q}$ is minimal, we obtain $Q \not\supset \bigcap_{Q' \in \mathcal{Q}_1(J)} Q'$ for any $Q \in \mathcal{Q}_2(J)$ and $Q \not\supset \bigcap_{Q' \in \mathcal{Q}_1(J)} Q'$ for any $Q \in \mathcal{Q}_3(J)$. Thus, by Lemma 18,

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

From (6) in Proposition 19, we obtain $\sqrt{(I : (I : J))} = \sqrt{(I : (I : J^\infty))}$. ∎

Example 26
For $I = (x^2) \cap (x^3, y^2) \cap (y)$ *and* $J = (x^2)$, $\sqrt{(I : (I : J^\infty))} = \bigcap_{P \in \mathrm{Ass}(I), J \subset P} P = (x)$.

4 Criteria for Primary Component and Prime Divisor

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

4.1 General Primary Component Criterion

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

Definition 27 ([5], Definition 24)
Let I and J be ideals. We say that J is saturated quotient invariant *of I if $(I : (I : J)^\infty) = J$.*

Example 28
Let $I = (x) \cap (x^2, y)$ and $J = (x)$. Then J is saturated quotient invariant of I since $(I : (I : J)^\infty) = (I : (x, y)^\infty) = (x)$.

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

Lemma 29 ([5], Lemma 25)
Let I be an ideal and J a proper ideal of $K[X]$. Then, the following conditions are equivalent.
(A) $J = IK[X]_S \cap K[X]$ for some multiplicatively closed set S.
(B) J is saturated quotient invariant of I.

Proof Let Q be a primary decomposition. Show (A) implies (B). From Proposition 23 (7),

$$(I : (I : IK[X]_S \cap K[X])^\infty) = \bigcap_{Q \in \mathcal{Q}, IK[X]_S \cap K[X] \subset IK[X]_{\sqrt{Q}} \cap K[X]} Q. \tag{10}$$

By Lemma 77, $IK[X]_S \cap K[X] \subset IK[X]_{\sqrt{Q}} \cap K[X]$ if and only if $Q \cap S = \emptyset$. Thus,

$$\bigcap_{Q \in \mathcal{Q}, IK[X]_S \cap K[X] \subset IK[X]_{\sqrt{Q}} \cap K[X]} Q = \bigcap_{Q \in \mathcal{Q}, Q \cap S = \emptyset} Q, \tag{11}$$

Combining (10), (11) and $IK[X]_S \cap K[X] = \bigcap_{Q \in \mathcal{Q}, Q \cap S = \emptyset} Q$ by Remark 4, we obtain $(I : (I : IK[X]_S \cap K[X])^\infty) = IK[X]_S \cap K[X]$.

Next, show (B) implies (A). From Proposition 23 (7),

$$(I : (I : J)^\infty) = \bigcap_{J \subset IK[X]_{\sqrt{Q}} \cap K[X]} Q = J. \tag{12}$$

Let $\mathcal{P} = \{ \sqrt{Q} \mid Q \in \mathcal{Q}, J \subset IK[X]_{\sqrt{Q}} \cap K[X] \}$. We may assume $\mathcal{P} \neq \emptyset$, otherwise $\mathcal{P} = \emptyset$ and $J = K[X]$. Then $\mathcal{P}$ is *an isolated set* (see Definition 74) since if $P' \in \mathrm{Ass}(I)$ and $P' \subset P$ for some $P \in \mathcal{P}$, then $J \subset IK[X]_P \cap K[X] \subset IK[X]_{P'} \cap K[X]$ and $P' \in \mathcal{P}$. Let $S = K[X] \setminus \bigcup_{P \in \mathcal{P}} P$. By Lemma 75, $IK[X]_S \cap K[X] = \bigcap_{Q \in \mathcal{Q}, \sqrt{Q} \in \mathcal{P}} Q = \bigcap_{J \subset IK[X]_{\sqrt{Q}} \cap K[X]} Q$. By (12), we obtain $IK[X]_S \cap K[X] = J$. ∎

Example 30
Let $I = (x) \cap (x^2, y)$ and $J = (x)$. Then J is saturated quotient invariant of I and $J = IK[X]_{(x)} \cap K[X]$.

Based on Lemma 29, we have the following criterion for primary component.

Theorem 31 (Criterion 1. [5], Theorem 26)
Let I be an ideal and P a prime divisor of I. For a P-primary ideal Q, if $Q \not\supset (I : P^\infty)$, then the following conditions are equivalent.
(A) Q is a P-primary component for some primary decomposition of I.
(B) $(I : P^\infty) \cap Q$ is saturated quotient invariant of I.

Proof Show (A) implies (B). Let $\mathcal{Q}$ be a primary decomposition. Let $\mathcal{P} = \{P' \in \mathrm{Ass}(I) \mid P \not\subset P' \text{ or } P' = P\}$ and $S = K[X] \setminus \bigcup_{P' \in \mathcal{P}} P'$. Then S is a multiplicatively closed set and $(I : P^\infty) \cap Q \subset IK[X]_S \cap K[X]$ since $(I : P^\infty) \cap Q = \bigcap_{Q' \in \mathcal{Q}, P \not\subset \sqrt{Q'}} Q' \cap Q$. For each $Q' \in \mathcal{Q}$ with $Q' \cap S = \emptyset$, there is $P' \in \mathcal{P}$ such that $\sqrt{Q'} \subset P'$, i.e. $\sqrt{Q'} \in \mathcal{P}$. Thus, $(I : P^\infty) \cap Q \supset IK[X]_S \cap K[X]$ and $(I : P^\infty) \cap Q = IK[X]_S \cap K[X]$. By Lemma 29, $IK[X]_S \cap K[X]$ is saturated quotient invariant of I.

Show (B) implies (A). By Lemma 29, there is a multiplicatively closed set S such that $(I : P^\infty) \cap Q = IK[X]_S \cap K[X]$. Let $\mathcal{Q}$ be a primary decomposition of I. We know $IK[X]_S \cap K[X] = \bigcap_{Q' \in \mathcal{Q}, Q' \cap S = \emptyset} Q'$. By the assumption, $Q \not\supset (I : P^\infty)$ and thus $(I : P^\infty) \cap Q$ has a P-primary component. Then neither $\bigcap_{Q' \in \mathcal{Q}, Q' \cap S \neq \emptyset} Q'$ nor $(I : P^\infty)$ has a P-primary component. Hence,

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

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

Example 32
Let $I = (x) \cap (x^2, y^2) \cap (x^3, y^3, z) \cap (y) \cap (x + 1, z)$ and $P = (x, y)$ in $\mathbb{Q}[x, y, z]$. Then, $(I : P^\infty) = (x) \cap (y) \cap (x + 1, z)$. We think the following two P-primary ideals.

- *$Q_1 = (x^2, y^2)$. Since $Q_1 \not\supset (I : P^\infty)$ and $(I : (I : ((I : P^\infty) \cap Q_1))^\infty) = (x) \cap (y) \cap (x + 1, z) \cap (x^2, y^2) = (I : P^\infty) \cap Q_1$, we obtain (x^2, y^2) is a P-primary component of I.*
- *$Q_2 = (x^2, x + y)$. Since $(I : (I : ((I : P^\infty) \cap Q_2))^\infty) = (x) \cap (y) \cap (x + 1, z) \neq (I : P^\infty) \cap Q_2$, we obtain $(x^2, x + y)$ is not a P-primary component of I.*

4.2 Other Criteria for Primary Component

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

4.2.1 Criterion for Isolated Primary Component:

If Q is a primary ideal whose radical is an isolated divisor P of an ideal I, then we don't need to compute $(I : P^\infty)$ in Theorem 31 since the P-primary component of I is the localization of I by P.

Theorem 33 (Criterion 2. [5], Theorem 27)
Let I be an ideal and P an isolated prime divisor of I. For a P-primary ideal Q, the following conditions are equivalent.
(A) Q is the isolated P-primary component of I.
(B) $(I : (I : Q)^\infty) = Q$.

Proof Show (A) implies (B). Let $S = K[X] \setminus P$. By Lemma 29, $Q = IK[X]_S \cap K[X]$ is saturated quotient invariant of I and thus $(I : (I : Q)^\infty) = Q$. Next, we show (B) implies (A). By Lemma 29, there is a multiplicatively closed set S s.t. $IK[X]_S \cap K[X] = Q$. Since Q is primary, $IK[X]_S \cap K[X]$ is the isolated P-primary component. ∎

Example 34
For $I = (x^2) \cap (x^3, y^2) \cap (y)$, a primary component $Q = (x^2)$ is isolated and $(I : (I : Q)^\infty) = (x^2) = Q$.

4.2.2 Criterion for Maximal Primary Component:

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

Definition 35
Let P be a prime divisor of I. We say P is maximal *if there is no prime divisor P' of I containing P properly.*

Example 36
For $I = (x) \cap (x^2, y^2) \cap (z^2)$ in $\mathbb{Q}[x, y, z]$, prime divisors $P_1 = (x, y)$ and $P_2 = (z)$ are maximal in $\mathrm{Ass}(I) = \{(x), (x, y), (z)\}$.

Theorem 37 (Criterion 3. [5], Theorem 29)
Let I be an ideal and P a maximal prime divisor of I. For P-primary ideal Q, the following conditions are equivalent.

(A) Q is a P-primary component of I.
(B) $(I : P^\infty) \cap Q = I$.

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

Example 38
Let $I = (x) \cap (x^2, y^2) \cap (z^2)$ and $P = (x, y)$ in $\mathbb{Q}[x, y, z]$. Then P is maximal in $\mathrm{Ass}(I)$ *and $Q = (x^2, y^2)$ is a P-primary component of I since $(I : P^\infty) \cap Q = (x) \cap (z^2) \cap (x^2, y^2) = I$.*

4.2.3 Criterion for Another General Primary Component:

The general case can be reduced to maximal case via localization by maximal independent set. A subset U of X is called a maximal independent set of I if $K[U] \cap I = 0$ and the cardinality of U is equal to the dimension of I (see [6] for its computation). Letting $S = K[U]^\times = K[U] \setminus \{0\}$, we obtain the following as a special case of Lemma 72.

Theorem 39 (Criterion 4. [5], Theorem 30)
Let I be an ideal and P a prime divisor of I. If U is a maximal independent set of P in X and Q is a P-primary ideal , then the following conditions are equivalent.

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

Example 40
For $I = (x) \cap (x^2, y) \cap (x^3, y^2, z)$, we obtain (x^2, y) is a primary component of both I and $I\mathbb{Q}[X]_{(x,y)} \cap \mathbb{Q}[X] = (x) \cap (x^2, y)$.

4.3 Additional Criterion for Prime Divisor

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

Theorem 41 (Criterion 5. [5], Theorem 31)
Let I be an ideal and P a prime ideal. Then, the following conditions are equivalent.
(A) $P \in \mathrm{Ass}(I)$.
(B) $P \supset (I : (I : P))$.
(C) $P \supset (I : (I : P^\infty))$.

Proof By Corollary 20, (A) is equivalent to (B). By Proposition 25,
$\sqrt{(I : (I : P))} = \sqrt{(I : (I : P^\infty))} = \bigcap_{P' \in \mathrm{Ass}(I), P \subset P'} P'$. Thus, equivalence between (A) and (C) is proved by the similar way of Corollary 20. ∎

Example 42
For $I = (x^2) \cap (x^4, y) \cap (x + 1)$ and a prime divisor $P = (x)$, we obtain $(I : (I : P)) = (x) \subset P$ and $(I : (I : P^\infty)) = (x^2) \cap (x^4, y) \subset P$.

Next, we devise another way to compute pseudo-primary components and criteria for isolated prime divisors based on the second saturated quotient.

Lemma 43 ([5], Lemma 32)
Let I be an ideal and P an isolated prime divisor of I. If $\overline{Q}$ is the minimal P-pseudo-primary component of I, then $(I : (I : P^\infty)^\infty) = \overline{Q}$.

Proof Let $\mathcal{Q}$ be a primary decomposition of I. By Proposition 23 (8),

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

Thus it is enough to show that the following statements are equivalent for each $Q \in \mathcal{Q}$.
(1-a) $P \subset \sqrt{IK[X]_{\sqrt{Q}} \cap K[X]}$.
(1-b) P is the unique isolated prime divisor which is contained in $\sqrt{Q}$.
Show (1-a) implies (1-b). As $\sqrt{IK[X]_{\sqrt{Q}} \cap K[X]} \subset \sqrt{Q}$, we know $P \subset \sqrt{Q}$. Then, suppose there is another isolated prime divisor P' contained in $\sqrt{Q}$. We obtain

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

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

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

∎

Example 44
For $I = (x) \cap (x^2, y^2) \cap (y+1)$ and $P = (x)$, we obtain $(I : (I : P^\infty)^\infty) = (x) \cap (x^2, y^2)$ is the minimal P-pseudo-primary component of I.

Using Lemma 43, we obtain the following criterion for isolated prime divisor.

Theorem 45 (Criterion 6. [5], Theorem 33)
Let I be an ideal and P a prime ideal containing I. Then, the following conditions are equivalent.
(A) P is an isolated prime divisor of I.
(B) $(I : (I : P^\infty)^\infty) \neq K[X]$.

Proof Show (A) implies (B). By Lemma 43, $(I : (I : P^\infty)^\infty) = \overline{Q} \neq K[X]$. Show ($B$) implies ($A$). By Proposition 23 (8),

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

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

Since each prime divisor of I contains I, Theorem 45 directly induces the following.

Corollary 46 (Criterion 7. [5], Corollary 34)
Let I be an ideal and P a prime divisor of I. Then,
(i) *P is isolated if $(I : (I : P^\infty)^\infty) \neq K[X]$,*
(ii) *P is embedded if $(I : (I : P^\infty)^\infty) = K[X]$.*

Example 47
Let $I = (x) \cap (x^2, y^2) \cap (y+1)$. For a prime divisor $P_1 = (x)$, $(I : (I : P^\infty)^\infty) = (x) \cap (x^2, y^2) \neq \mathbb{Q}[X]$ and P_1 is isolated. For a prime divisor $P_2 = (x, y)$, $(I : (I : P^\infty)^\infty) = \mathbb{Q}[X]$ and P_2 is embedded.

5 Local Primary Algorithm

In this section, we devise Local Primary Algorithm (LPA) which computes P-primary component of I. Our method applies different procedures for two cases; isolated and embedded. Algorithm 1 shows the outline of LPA. Its termination comes from Proposition 48. We remark that, for given prime divisors disjoint from a multiplicatively closed set S, we can compute all primary components disjoint from S by LPA. Then their intersection gives the localization by S.

5.1 Generating Primary Component

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

Proposition 48 ([2], Section 4. [10], Remark 10)
Let I be an ideal and P a prime divisor of I. For any positive integer m, $I + P^m$ is P-hull-primary, and for a sufficiently large integer m, $\mathrm{hull}(I + P^m)$ is a P-primary component appearing in a primary decomposition of I.

Example 49
For $I = (x) \cap (x^2, y) \cap (x^3, y^2, z)$ and $P = (x, y)$, we obtain $I + P^3 = (x^3, x^2y, xy^2, y^3, x^2z, xyz)$ and $\mathrm{hull}(I + P^3) = (x^2, xy, y^3)$ is a P-primary component of I.

We can use Criteria for Primary Component to check m is large enough or not. If P is an isolated prime divisor, then the component is computed directly by using the second saturated quotient. By Lemma 16 and Lemma 43, we obtain the following theorem. To compute equidimensional hull, we can use regular sequence (see Proposition 12) or maximal independent set (see Lemma 58).

Theorem 50 ([5], Theorem 36)
Let I be an ideal and P an isolated prime divisor of I. Then

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

is the isolated P-primary component of I.

Example 51
For $I = (x^2) \cap (x^3, y^2) \cap (y + 1)$ and $P = (x)$, the isolated P-primary component is $\mathrm{hull}((I : (I : P^\infty)^\infty)) = \mathrm{hull}((x^2) \cap (x^3, y^2)) = (x^2)$.

Algorithm 1 General Frame of Local Primary Algorithm

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

1: **if** P is a prime divisor of I (**Criterion 5**) **then**
2: **if** P is isolated (**Criteria 6,7**) **then**
3: $\overline{Q} \leftarrow$ the minimal P-pseudo-primary component of I (**Lemma 43**)
4: $Q \leftarrow \mathrm{hull}(\overline{Q})$ (**Theorem 50**)
5: **return** Q is the isolated P primary component
6: **else**
7: $m \leftarrow 1$, $Q \leftarrow K[X]$
8: **while** Q is not primary component of I (**Criteria 1,3,4**) **do**
9: $\overline{Q} \leftarrow$ a P-hull-primary ideal related to m (**Proposition 48, Lemma 54**)
10: $Q \leftarrow \mathrm{hull}(\overline{Q})$
11: $m \leftarrow m + 1$
12: **end while**
13: **return** Q is an embedded P-primary component
14: **end if**
15: **else**
16: **return** "P is not a prime divisor"
17: **end if**

5.2 Techniques for Improving LPA

We introduce practical techniques for implementing LPA.

5.2.1 Another Way of Generating Primary Component

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

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

Lemma 52 ([5], Lemma 37)
Let $\mathcal{Q}$ be a primary decomposition of I and $Q \in \mathcal{Q}$. If $\sqrt{Q}$-hull-primary ideal Q' satisfies $I \subset Q' \subset Q$, then $(\mathcal{Q} \setminus \{Q\}) \cup \{\mathrm{hull}(Q')\}$ is another primary decomposition of I.

Proof By Lemma 81, we obtain $I \subset Q' \subset \mathrm{hull}(Q') \subset Q$. Since $I \cap \mathrm{hull}(Q') = I$ and $Q \cap \mathrm{hull}(Q') = \mathrm{hull}(Q')$, we obtain

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

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

Example 53
Let $I = (x) \cap (x^2, y) \cap (z)$, $Q' = (x^2, xy, y^2) \cap (x^2, xy, y^3, z+1)$ and $P = (x, y)$. Then, Q' is P-hull-primary. For a primary component $Q = (x^2, y)$, we obtain $I \subset Q' \subset Q$ and $\mathrm{hull}(Q') = (x^2, xy, y^2)$ is a P-primary component of I.

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

Lemma 54 ([5], Lemma 38)
For any positive integer m, $I + P_G^{[m]}$ is P-hull-primary, and for a sufficiently large m, $\mathrm{hull}(I + P_G^{[m]})$ is a P-primary component appearing in a primary decomposition of I if P is a prime divisor of I.

Proof As $\sqrt{P_G^{[m]}} = P$ and $\sqrt{I + P} = \sqrt{I + P_G^{[m]}} = P$, $I + P_G^{[m]}$ is P-hull-primary. By Proposition 48, $\mathrm{hull}(I + P^m)$ is a P-primary component of I for a sufficiently large m. Since $I \subset I + P_G^{[m]} \subset I + P^m \subset \mathrm{hull}(I + P^m)$, $\mathrm{hull}(I + P_G^{[m]})$ is a P-primary component by Lemma 52. ∎

Example 55
For $I = (x) \cap (x^2, y) \cap (x^3, y^2, z)$ and $P = (G) = (x, y)$, we obtain $I + P_G^{[3]} = (x^3, xy^2, y^3, x^2z, xyz)$ and $\mathrm{hull}(I + P_G^{[3]}) = (x^2, xy, y^3)$ is a P-primary component of I.

5.2.2 Regular Sequence Computation for Pseudo-Primary Ideal

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

Lemma 56
Let I be a P-pseudo-primary ideal and $u = \{f_1, \ldots, f_c\}$ a regular sequence in P. Then, for efficiently large integers $m_1, \ldots, m_c$, $\{f_1^{m_1}, \ldots, f_c^{m_c}\}$ is a regular sequence in I.

Proof By Theorem 26 in [9], $\{f_1^{m_1}, \ldots, f_c^{m_c}\}$ is a regular sequence for any positive integers $m_1, \ldots, m_c$. Since I is P-pseudo-primary, it follows that $\sqrt{I} = P$. Thus, for efficiently large integer $m_1, \ldots, m_c$, $\{f_1^{m_1}, \ldots, f_c^{m_c}\} \subset I$ and it is a regular sequence in I. ∎

Since $\sqrt{(I : (I : P^\infty)^\infty)} = P$ if P is isolated, we obtain the following Corollary. From $\mathrm{codim}(P) = \mathrm{codim}((I : (I : P^\infty)^\infty))$ and Lemma 12, we can compute the equidimensional hull $\mathrm{hull}((I : (I : P^\infty)^\infty))$ by using a regular sequence in P.

Corollary 57
Let I be an ideal and P its isolated prime divisor. Let $u = \{f_1, \ldots, f_c\}$ be a regular sequence in P. Then, for efficiently large integer m, $\{f_1^m, \ldots, f_c^m\}$ is a regular sequence in $(I : (I : P^\infty)^\infty)$.

5.2.3 Equidimensional Hull Computation with MIS

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

Lemma 58 ([5], Lemma 39)
Let I be a P-hull-primary ideal. For a maximal independent set U of P, $\mathrm{hull}(I) = IK[X]_{K[U]^\times} \cap K[X]$.

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

Example 59
For $I = (x) \cap (x^2, y)$ and $P = (x)$ in $\mathbb{Q}[X] = \mathbb{Q}[x, y]$, we obtain $U = \{y\}$ is a maximal independent set of P. Then, $\mathrm{hull}(I) = (x) = I\mathbb{Q}[X]_{\mathbb{Q}[U]^\times} \cap \mathbb{Q}[X]$.

6 Further Discussion of Local Primary Algorithm

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

First, we introduce a new criterion for prime divisors using maximal independent set instead of double ideal quotient.

Proposition 60 (Criterion 8)
Let I be an ideal and P a prime ideal in $K[X]$. Then the following statements are equivalent.

1. $P \in \mathrm{Ass}(I)$.
2. $(I' : P^\infty) \neq I'$, *where* $I' = IK[X]_{K[U]^\times} \cap K[X]$ *for a maximal independent set U of P.*

Proof Let $\mathcal{Q}$ be a primary decomposition of I. To prove that (1) implies (2), we remark that $P \in \mathrm{Ass}(I)$ leads $P \in \mathrm{Ass}(I')$ from Lemma 72 and $P \cap K[U]^\times = \emptyset$. Thus, we obtain that $(I' : P^\infty) \neq I'$ since $P \notin \mathrm{Ass}((I' : P^\infty))$. Next, we show (2) implies (1). Since $(I' : P^\infty) \neq I'$, there is a prime divisor $P' \in \mathrm{Ass}(I')$ containing P. Then $P' \cap K[U]^\times = \emptyset$ and $\dim(P') \leq \dim(P) = \#U$. From Lemma 72, $P' \in \mathrm{Ass}(I)$ and thus $\dim(P') \geq \#U$. Hence, $\dim(P) = \dim(P')$ and $P = P' \in \mathrm{Ass}(I)$. ∎

Example 61
Let $I = (x^2) \cap (x^3, y)$ and $P = (x)$ in $\mathbb{Q}[X] = \mathbb{Q}[x, y]$. Then, $U = \{y\}$ is the maximal independent set of P and $I' = I\mathbb{Q}[X]_{\mathbb{Q}[U]^\times} \cap \mathbb{Q}[X] = (x^2)$. Since $(I' : P^\infty) = \mathbb{Q}[X] \neq I'$, we get $P \in \mathrm{Ass}(I)$.

Next, we introduce a *P-pseudo-descending chain* to devise a generalized splitting tool and a new criterion for isolated prime divisors. It is a generalization of P^m and $P_G^{[m]}$ in [5].

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

Example 63
As an easy example, $P \supset P^2 \supset P^3 \supset \cdots$ is a P-pseudo-descending chain. For a generator G of P, $P_G^{[1]} \supset P_G^{[2]} \supset P_G^{[3]} \supset \cdots$ is a P-pseudo-descending chain since $P_G^{[m]}$ is P-pseudo-primary and $PP_G^{[m]} \supset P_G^{[m+1]}$ for every m.

Remark 64
We remark that a P-pseudo-descending chain is not always P-filtration i.e. it does not always satisfy the other inclusion $PJ_m \subset J_{m+1}$.

We can use a P-pseudo-descending chain to generate P-primary component as Lemma 65, a generalization of Proposition 48 and Lemma 54.

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

Proof Let Q be a P-primary component of I. Since $K[X]$ is Noetherian, there is an efficiently large integer m s.t. $P^m \subset Q$. As $P^m \supset P^{m-1}J_1 \supset P^{m-2}J_2 \supset \cdots \supset PJ_{m-1} \supset J_m$, it follows that $I \subset I + J_m \subset Q$. Here, $\sqrt{I + J_m} = \sqrt{\sqrt{I} + P} = P$ and thus $I + J_m$ is P-pseudo-primary, in particular, P-hull-primary. From Lemma 52, we obtain $\mathrm{hull}(I + J_m)$ is a P-primary component of I. Next, we show the second statement. If $\mathrm{hull}(I + J_m)$ is a P-primary component of I for some m, then it follows that $I \subset I + J_{m+1} \subset I + J_m \subset \mathrm{hull}(I + J_m)$. Thus, $\mathrm{hull}(I + J_{m+1})$ is a P-primary component of I from Lemma 52. ∎

Example 66
Let $I = (x^2, xy)$, $P = (x, y)$ and $J_m = (x^m, y^m)$. We obtain $\mathrm{hull}(I + J_m) = (x^2, xy, y^m)$ *is a P-primary component if $m \geq 2$.*

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

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

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

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

Proof By Lemma 83, $I = (I : P^\infty) \cap (I + P^m)$ for an efficiently large integer m. As $J_m \subset P^m$, it follows that

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

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

Example 68
Let $I = (x^2, xy)$, $P = (x, y)$ and $J_m = (x^m, y^m)$. We obtain $I = (I : P^\infty) \cap (I + J_2) = (x) \cap (x^2, xy, y^2)$ and (x^2, xy, y^2) is a P-primary component of I.

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

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

1. *P is an isolated prime divisor of I.*
2. $\mathrm{hull}(I + J_m) = \mathrm{hull}(I + J_{m+1})$.

Proof First, we show (1) implies (2). By Lemma 65, $\mathrm{hull}(I+J_{m+1})$ is also a P-primary component of I. Since P is isolated, the P-primary component is unique and $\mathrm{hull}(I + J_m) = \mathrm{hull}(I + J_{m+1})$. Second, we show (2) implies (1). Let $R = K[X]_P/IK[X]_P$. Since $I + J_m$ is P-hull-primary, it follows that $\mathrm{hull}(I + J_m) = (I + J_m)K[X]_P \cap K[X]$ and thus $\mathrm{hull}(I + J_m)R = J_mR$. As $\mathrm{hull}(I + J_m) = \mathrm{hull}(I + J_{m+1})$, we get $J_mR = J_{m+1}R$. Thus, $J_m \supset PJ_m \supset J_{m+1}$ and it follows that $J_mR \supset PJ_mR \supset J_{m+1}R = J_mR$, hence, $J_mR = PJ_mR$. Since J_mR is finitely generated $K[X]_P$-module, we obtain $J_mR = 0$ by Nakayama's Lemma. Thus, $J_mK[X]_P = IK[X]_P$ and $P \in \mathrm{Ass}(\sqrt{I})$, otherwise, $IK[X]_P$ has two or more prime divisors. Therefore, P is isolated. ∎

Example 70
Let $I = (x^2) \cap (x^3, y)$. For $P_1 = (x)$, it follows that $\mathrm{hull}(I + P_1^2) = \mathrm{hull}(I + P_1^3) = (x^2)$ *is a P_1-primary component. Thus, P_1 is the isolated prime divisor of I. On the other hand, for $P_2 = (x, y)$ and $J_m = (x^m, y^m)$,* $\mathrm{hull}(I + J_3) = (x^3, x^2y, y^3)$ *is a P_2-primary component and hull$(I + J_3) \supsetneq$* $\mathrm{hull}(I + J_4) = (x^3, x^2y, y^4)$*; thus P_2 is embedded.*

Remark 71
An integer m s.t. $\mathrm{hull}(I+J_m)$ *is a P-primary component of I may be smaller than m' s.t.* $\mathrm{hull}(I+P^{m'})$ *is a P-primary component of I. Thus, we may compute a primary component more easily by* $\mathrm{hull}(I + P_G^{[m]})$.

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

7 Experiments and Observations

We made an implementation on the computer algebra system Risa/Asir [11] and apply it to several examples as experiments. We revisited old examples in [5], $I_1(n)$ and $A_{k,m,n}$. The former $I_1(n) = (x^2) \cap (x^4, y) \cap (x^3, y^3, (z + 1)^n + 1)$ is an ideal whose embedded primary components are hard to compute. If n is considerable large, it is difficult to compute a full primary decomposition of $I_1(n)$ though the isolated divisor $P_1 = (x)$ can be detected pretty easily. The latter $A_{k,m,n}$ defined in [13] is more valuable for mathematics and its primary decomposition has important meanings in Computer Algebra for Statistics. We newly considered $T_1, \ldots, T_{10}$ that appear in [7] for benchmarks of primary decomposition. We describe the more details of ideals in A.2. Timings are measured on a PC with Intel Core i7-8700B CPU with 32GB memory.

Algorithm 2 Local Primary Algorithm Without Double Ideal Quotient

Input: I: an ideal, P: a prime ideal in $K[X]$
Output: • a P-primary component if P is a prime divisor
• "P is not a prime divisor" otherwise

1: $U \leftarrow$ a Maximal Independent Set of P, $I' \leftarrow IK[X]_{K[U]^\times} \cap K[X]$
2: $G \leftarrow \{f_1, \ldots, f_s\}$ a generator of P, $m \leftarrow 1$
3: **if** $(I' : P^\infty) = I'$ **then**
4: **return** "P is not a prime divisor " (**Criterion 8**)
5: **end if**
6: **while** $(I' : P^\infty) \cap (I' + P_G^{[m]}) \neq I'$ **do**
7: $m \leftarrow m + 1$ (**Proposition 67**)
8: **end while**
9: $Q_m \leftarrow \mathrm{hull}(I' + P_G^{[m]}) = (I' + P_G^{[m]})K[X]_{K[U]^\times} \cap K[X]$ (**Lemma 58**)
10: $Q_{m+1} \leftarrow \mathrm{hull}(I' + P_G^{[m+1]}) = (I' + P_G^{[m+1]})K[X]_{K[U]^\times} \cap K[X]$
11: **if** $Q_m = Q_{m+1}$ **then**
12: **return** "Q_m is the isolated P-primary component of I " (**Criterion 9**)
13: **else**
14: **return** "Q_m is an embedded P-primary component of I " (**Criterion 9**)
15: **end if**

Now, we explain the details of Local Primary Algorithms (LPAs). From Proposition 12, the primitive LPA use *double ideal quotient* and *regular sequence* to compute *equidimensional hull*. To compute a regular sequence in $I + P_G^{[m]}$ and that in $(I : (I : P^\infty)^\infty)$ efficiently, we use Lemma 56 and Corollary 57 respectively. As improved versions, LPA-$P_G^{[m]}$ is an implementation based on Lemma 54 and LPA-MIS is one from Lemma 58 and Criteria 3, 4. Both methods are implemented in LPA-($P_G^{[m]}$+MIS). The new algorithm LPA-($P_G^{[m]}$+MIS) without DIQ is based on Algorithm 2. Here, as a reference, we show the timings of a full primary decomposition function `noro_pd.syci_dec` in Table 6.

In all Figures, the horizontal axis shows isolated or embedded prime divisors and the vertical axis represents the timing (in seconds) of each prime divisor. In particular, the embedded prime divisors are in order of decreasing dimension.

7.1 Computation of Isolated Components

First, we apply LPAs to isolated primary components. In Table 1 and Table 2, we can see LPAs have clearly effectiveness by their specialities. We call an algorithm *stable* for an ideal if the *statistical standard deviation* of timing data for their prime divisors is small. Figure 1 and Table 3 show that LPA is stable for T_1 since the the statistical standard deviation is 4.17, which is much smaller than those of LPA-MIS and LPA-($P_G^{[m]}$+MIS). On the other hand, both LPA-MIS and LPA-($P_G^{[m]}$+MIS) without DIQ take much time for some cases and are unstable since the statistical standard deviations are over 100 times of that of LPA. Also, we can see its instability in Figures 2 and 3, where we limit the maximum to 35 seconds. The main reason is that MIS-localization becomes very time-consuming for specific ideals and prime ideals. However, when MIS-localization is efficient, timings of LPA-MIS and LPA-($P_G^{[m]}$+MIS) without DIQ are much faster than those of LPA. There are almost no difference between timings of LPA-MIS and LPA-($P_G^{[m]}$+MIS) without DIQ since MIS-localization is very effective and it can reduce the timings of other parts. As a summary of analysis for isolated examples,

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

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

Table 1: Local Primary Algorithm (Isolated)

Ideals (# of isolated components)	LPA	LPA-MIS	LPA-($P_G^{[m]}$+MIS) w/o DIQ
T_1 (49)	100	73.4	75.5
T_2 (15)	0	0	0
T_3 (47)	97.8	82.9	82.9
T_4 (40)	100	95.0	95.0
T_5 (14)	100	71.4	71.4
T_6 (48)	100	100	100
T_7 (55)	100	89.0	90.9
T_8 (37)	91.8	67.5	67.5
T_9 (15)	100	26.6	40.0
T_{10} (76)	100	43.4	46.0

Table 2: Comparison among LPAs (the ratios of isolated primary components which each LPA could compute more efficiently than the specified full primary decompositions.)

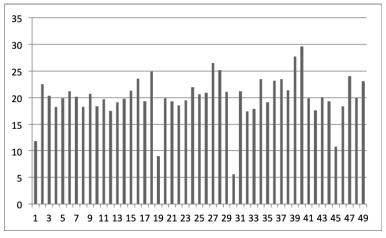


Fig. 1: LPA (49 isolated prime divisors of T_1)

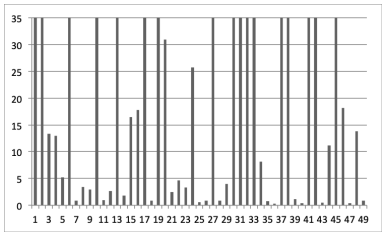


Fig. 2: LPA-MIS (49 isolated prime divisors of T_1)

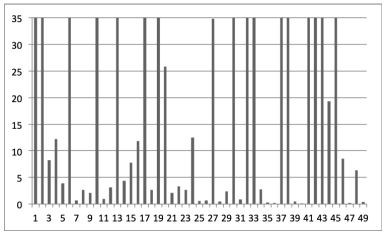


Fig. 3: LPA-($P_G^{[m]}$+MIS) without DIQ (49 isolated prime divisors of T_1)

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

Table 3: The statistical standard deviations of timing data for isolated prime divisors, where we limit the maximum to 1200 seconds

7.2 Computation of Embedded Components

In Table 4, the primitive LPA is not practical for some examples since the cost of computing hull($I + P^m$) is much high. Comparing LPA and LPA-$P_G^{[m]}$ (also LPA-MIS and LPA-($P_G^{[m]}$+MIS)), we can see the technique $P_G^{[m]}$-products is effective for most cases. As algorithms using MIS-localization, LPA-($P_G^{[m]}$+MIS) and LPA-($P_G^{[m]}$+MIS) without DIQ have good effectivenesses by their specialities for many cases, for examples, $(I_1(n), P_{14})$, $(A_{2,4,4}, P_{15})$, $(A_{2,3,7}, P_{16})$, (T_1, P_{17}), (T_4, P_{21}), (T_7, P_{24}), (T_8, P_{25}), (T_{10}, P_{27}) and so on. From Table 4, we can see MIS-technique is efficient for many cases. However, there are some examples s.t. MIS-localization is not efficient, for instance, (T_1, P_{18}) and (T_3, P_{20}). As a consideration of the ration of such non-efficient case, in Table 5, we can see both LPA-($P_G^{[m]}$+MIS) and LPA-($P_G^{[m]}$+MIS) are effective for 96.6% of embedded prime divisors of T_1 i.e. MIS-localization is efficient for *most* embedded prime divisors of T_1. In Figures 4,5 and 7, we can see LPAs using MIS are unstable due to MIS-localization, comparing LPA-$P_G^{[m]}$. Same as isolated components, there are almost no difference between timings of LPA-($P_G^{[m]}$+MIS) and LPA-($P_G^{[m]}$+MIS) without DIQ since MIS-localization is much powerful and we can ignore the timings for computation of DIQ. In summary,

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

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

Table 4: Local Primary Algorithm (Embedded)

Ideals (# of embedded components)	LPA-$P_G^{[m]}$	LPA-($P_G^{[m]}$+MIS)	LPA-($P_G^{[m]}$+MIS) w/o DIQ
T_1 (120)	41.6	96.6	96.6

Table 5: Comparison of LPAs (the ratios of embedded primary components which each LPA could compute more efficiently than the specified full primary decomposition of T_1)

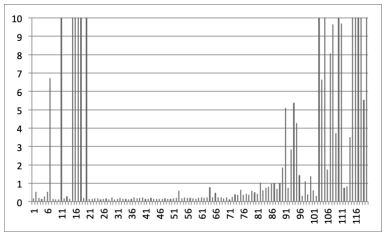


Fig. 4: LPA-($P_G^{[m]}$+MIS)
(120 embedded prime divisors of T_1)
upper limit: 10 seconds

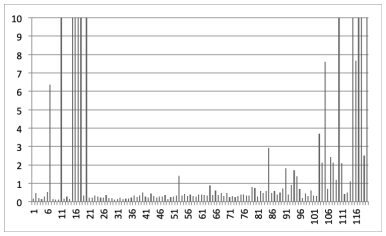


Fig. 5: LPA-($P_G^{[m]}$+MIS) w/o DIQ
(120 embedded prime divisors of T_1)
upper limit: 10 seconds

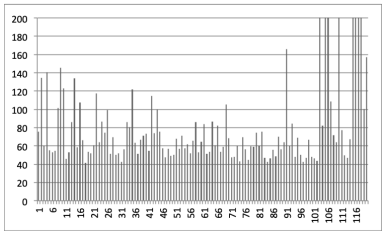


Fig. 6: LPA-$P_G^{[m]}$
(120 embedded prime divisors of T_1)
upper limit: 200 seconds

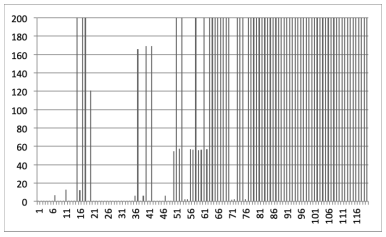


Fig. 7: LPA-MIS
(120 embedded prime divisors of T_1)
upper limit: 200 seconds

Ideals \ Algorithms	full primary decomposition (`noro_pd.syci_dec`)
$I_1(100)$	0.28
$I_1(200)$	11.3
$I_1(300)$	66.7
$I_1(400)$	167
$I_1(500)$	73.3
$A_{2,4,4}$	3.42
$A_{2,3,7}$	31.2
$A_{3,4,5}$	> 7200
T_1	62.7
T_2	30.0
T_3	63.9
T_4	35.0
T_5	49.8
T_6	5.58
T_7	261
T_8	1.82
T_9	5.24
T_{10}	324

Table 6: The timings of full primary decompositions (Reference)

7.3 Summary on Computational behavior

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

8 Conclusion and Future Work

In commutative algebra and algebraic geometry, the operation of "localization by a prime ideal" is widely known as a basic tool. In the paper, we focus on computing a primary component from only its prime divisor and propose a new effective localization Local Primary Algorithm (LPA). It mainly uses double ideal quotient (DIQ) (and its variants), and localization by maximal independent set (MIS). As an enhanced full paper version of [5], this paper contains detailed proofs, additional examples and new algorithms. Moreover, we took benchmarks for many examples to examine the effectiveness of LPA coming from its speciality. In the additional discussion, we invent another algorithm using a well-known splitting tool and maximal independent set instead of DIQ to compare it and the original LPAs. From experiments, we can see MIS-localization is very effective for many cases, however, it is *unstable* and there are some examples which are very time-consuming. We conclude that effectiveness of the LPAs depends on ideals and it would be better, at the moment, to apply them in parallel.

In future work, to make our LPAs very practical we shall continue to improve it through obtaining timing data for a lot of larger examples. In particular, we need to invent effective algorithms to compute double ideal quotient and MIS-localization. To solve it, we can apply so-called *modular techniques* using computations over finite fields for those over the rational field by Chinese Remainder Theorem and rational reconstruction. Since intermediate coefficient growth does not happen over a finite field, it is expected to reduce time of computation over the rational field dramatically. The first author just reported his first attempt of such modular techniques in the recent paper ([4]).

Another work shall be to apply our primary component criteria to *probabilistic or inexact* methods for primary decomposition, such as numerical ones. Probabilistic or inexact ways may have low computational costs but low accuracy for outputs. Hence, our criteria using double ideal quotient can guarantee their outputs. For example, we are thinking to combine our LPAs and Numerical Primary Decomposition in [8] to compute possible prime divisors and primary components.

Acknowledgements

The authors are grateful to Masayuki Noro for technical assistance with the computer experiments and coding on Risa/Asir. They are also thankful to Gerhard Pfister for his helpful comments on an earlier version of this paper. Finally, they thank the anonymous referees for their valuable comments and suggestions to improve this paper.

References

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

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

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

[4] Ishihara Y.: Modular Techniques for Effective Localization and Double Ideal Quotient. In Proceedings of the 45th International Symposium on Symbolic and Algebraic Computation (ISSAC '20). ACM, 265-272 (2020)

[5] Ishihara Y., Yokoyama K.: Effective Localization Using Double Ideal Quotient and Its Implementation. In: Gerdt V., Koepf W., Seiler W., Vorozhtsov E. (eds) Computer Algebra in Scientific Computing. CASC 2018. Lecture Notes in Computer Science, vol 11077. Springer, Cham, 272-287 (2018)

[6] Greuel, G.-M., Pfister, G.: A Singular Introduction to Commutative Algebra. Springer, Heidelberg (2002)

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

[8] Leykin, A.: Numerical Primary Decomposition. In Proceedings of the twenty-first International Symposium on Symbolic and Algebraic Computation (ISSAC '08). ACM, 165-172 (2008)

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

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

[11] The Risa/Asir developing team: Risa/Asir. A computer algebra system. http://www.math.kobe-u.ac.jp/Asir

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

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

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

A Fundamental Lemmas and their Proofs (Appendix)

A.1 Lemmas and Definitions

The following lemma is an easy but fundamental criterion for primary component using localization.

Lemma 72 ([5], Lemma 4)
Let I be an ideal and P its prime divisor. If S is a multiplicatively closed set with $P \cap S = \emptyset$ and Q is a P-primary ideal, then the following conditions are equivalent.
(A) *Q is a primary component of I*
(B) *Q is a primary component of $IK[X]_S \cap K[X]$*

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

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

Example 73
For $I = (x^2, xy) \subset K[X] = K[x, y]$, we obtain that (x) is the isolated primary component of both I and $IK[X]_{(x)} \cap K[X] = (x)$.

We define a special subset of $\mathrm{Ass}(I)$, which has a good relationship to localization. The localization by an isolated set can be expressed as intersection of primary components whose prime divisors are in the isolated set.

Definition 74 ([1], Chapter 4)
Let I be an ideal. A subset $\mathcal{P}$ of $\mathrm{Ass}(I)$ *is said to be* isolated *if it satisfies the following condition: for a prime divisor $P' \in \mathrm{Ass}(I)$, if $P' \subset P$ for some $P \in \mathcal{P}$, then $P' \in \mathcal{P}$.*

Lemma 75 ([1], Theorem 4.10)
Let I be an ideal and $\mathcal{P}$ an isolated set contained in $\mathrm{Ass}(I)$. *For a multiplicatively closed set $S = K[X] \setminus \bigcup_{P \in \mathcal{P}} P$ and a primary decomposition $\mathcal{Q}$ of I, $IK[X]_S \cap K[X] = \bigcap_{Q \in \mathcal{Q}, \sqrt{Q} \in \mathcal{P}} Q$.*

Example 76
For $I = (x^2(x+1), x(x+1)y) \subset K[X] = K[x, y]$, $\mathcal{P} = \{(x), (x, y)\}$ is an isolated subset of $\mathrm{Ass}(I) = \{(x), (x+1), (x, y)\}$. *Let $S = K[X] \setminus \bigcup_{P \in \mathcal{P}} P$. Then, $IK[X]_S \cap K[X] = (x) \cap (x^2, y)$.*

The following lemma tells us when primary component intersects a multiplicatively closed set. It is used to prove Lemma 29, a criterion for localization.

Lemma 77 ([5], Lemma 7)
Let $\mathcal{Q}$ be a primary decomposition of I and $Q \in \mathcal{Q}$. For a multiplicatively closed set S, the following conditions are equivalent.
(*A*) $IK[X]_S \cap K[X] \subset IK[X]_{\sqrt{Q}} \cap K[X]$.
(*B*) $Q \cap S = \emptyset$.

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

Example 78
For $I = (x) \cap (x+1) \cap (x^2, y) \subset \mathbb{Q}[X] = \mathbb{Q}[x, y]$, let $S = \mathbb{Q}[X] \setminus (x, y)$. Then, $I\mathbb{Q}[X]_S \cap \mathbb{Q}[X] \subset I\mathbb{Q}[X]_{\sqrt{(x)}} \cap \mathbb{Q}[X]$ and $(x) \cap S = \emptyset$. On the other hand, $I\mathbb{Q}[X]_S \cap \mathbb{Q}[X] \not\subset I\mathbb{Q}[X]_{\sqrt{(x+1)}} \cap \mathbb{Q}[X]$ and $(x+1) \cap S \neq \emptyset$.

The following lemma tells that primary ideal has a similar property to one of prime ideal.

Lemma 79 ([5], Lemma 16)
Let I and J be ideals. Let Q be a primary ideal. If $IJ \subset Q$ and $J \not\subset \sqrt{Q}$, then $I \subset Q$. In particular, if $I \cap J \subset Q$ and $J \not\subset \sqrt{Q}$, then $I \subset Q$.

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

Example 80
Let $I = (x)$, $J = (x+1)$ and $Q = (x, y^2)$. Then, $I \cap J \subset (x(x+1)) \subset (x, y^2) = Q$ and $J = (x+1) \not\subset \sqrt{Q} = (x, y)$. Thus, $I = (x) \subset Q = (x, y^2)$.

Hull-primary ideal has a similar property to one of primary ideal as follows.

Lemma 81 ([5], Lemma 17)
Let I be a P-hull-primary and Q a P-primary ideal. If $I \subset Q$, then $\mathrm{hull}(I) \subset Q$.

Proof Let $\mathcal{Q}$ be a primary decomposition of I and $J = \bigcap_{Q' \in \mathcal{Q}, Q' \neq \mathrm{hull}(I)} Q'$. Then $I = \mathrm{hull}(I) \cap J \subset Q$ and $J \not\subset P$. Since Q is P-primary, we obtain $\mathrm{hull}(I) \subset Q$ by Lemma 79. ∎

Example 82
Let $I = (x^2) \cap (x^3, y) \cap (x+1, y+1)$ and $Q = (x)$. Then, $I \subset Q$ and $\mathrm{hull}(Q) = (x^2) \subset Q$.

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

Lemma 83 ([14], Proposition 3.53)
Let I and J be ideals. Then, for a sufficiently large integer m,

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

Example 84
For $I = (x^2, xy)$ and $J = (x, y)$,

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

Also, we recall the famous Prime Avoidance Lemma.

Lemma 85 ([1], Proposition 1.11)
(i) *Let $P_1, \ldots, P_m$ be prime ideals and let I be an ideal contained in $\bigcup_{i=1}^{m} P_i$. Then, $I \subset P_i$ for some i.*
(ii) *Let $I_1, \ldots, I_m$ be ideals and let P be a prime ideal containing $\bigcap_{i=1}^{m} I_i$. Then $P \supset I_i$ for some i. If $P = \bigcap_{i=1}^{m} I_i$, then $P = I_i$ for some i.*

Finally, We add a proof of Lemma 18 in Sect. 2.2 as follows.

Lemma 18 ([5], Lemma 19)
Let I and J be ideals, Q a primary ideal and $\mathcal{Q}$ a primary decomposition of I. Then,

$$(Q : J) = \begin{cases} Q & (J \not\subset \sqrt{Q}), \\ K[X] & (J \subset Q), \\ \sqrt{Q}\text{-primary ideal properly containing } Q & (J \not\subset Q, J \subset \sqrt{Q}), \end{cases} \tag{1}$$

$$(Q : J^{\infty}) = \begin{cases} Q & (J \not\subset \sqrt{Q}), \\ K[X] & (J \subset \sqrt{Q}), \end{cases} \tag{2}$$

$$(I : J) = \bigcap_{Q \in \mathcal{Q}, J \not\subset \sqrt{Q}} Q \cap \bigcap_{Q \in \mathcal{Q}, J \not\subset Q, J \subset \sqrt{Q}} (Q : J), \tag{3}$$

$$(I : J^{\infty}) = (I : \sqrt{J}^{\infty}) = \bigcap_{Q \in \mathcal{Q}, J \not\subset \sqrt{Q}} Q. \tag{4}$$

Proof First, (1) can be proved directly from a remark before Proposition 3.56 in [14]. Second, we show (2). We note that $J \not\subset \sqrt{Q}$ implies $J^m \not\subset \sqrt{Q}$ for any positive integer m, and thus $(Q : J^m) = Q$ from (1). Since $K[X]$ is Noetherian, $(Q : J^{\infty}) = (Q : J^m)$ for a sufficiently large m. Thus, we obtain $(Q : J^{\infty}) = Q$ if $J \not\subset \sqrt{Q}$. If $J \subset \sqrt{Q}$, then $J^m \subset Q$ for a sufficiently large m and $(Q : J^{\infty}) = (Q : J^m) = K[X]$ from (1). Third, we prove (3). From $I = \bigcap_{Q \in \mathcal{Q}} Q$ and (1), we obtain

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

Finally, we show (4). From $I = \bigcap_{Q \in \mathcal{Q}} Q$ and (1), we obtain

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

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

A.2 Ideals and Prime Ideals in Experiments

$$
\begin{aligned}
I_1(n) =&(x^2) \cap (x^4, y) \cap (x^3, y^3, (z+1)^n + 1) \subset \mathbb{Q}[x, y, z].\\
A_{3,4,5} =&((x_{12}x_{23} - x_{13}x_{22})x_{31} - x_{11}x_{32}x_{23} + x_{11}x_{33}x_{22} + (x_{13}x_{32} - x_{12}x_{33})x_{21},\\
&(x_{13}x_{32} - x_{12}x_{33})x_{24} + (-x_{14}x_{32} + x_{12}x_{34})x_{23} + (x_{14}x_{33} - x_{13}x_{34})x_{22},\\
&(x_{14}x_{33} - x_{13}x_{34})x_{25} + (-x_{15}x_{33} + x_{35}x_{13})x_{24} + (x_{15}x_{34} - x_{35}x_{14})x_{23},\\
&(x_{42}x_{23} - x_{43}x_{22})x_{31} - x_{41}x_{32}x_{23} + x_{41}x_{33}x_{22} + (x_{43}x_{32} - x_{42}x_{33})x_{21},\\
&(x_{43}x_{32} - x_{42}x_{33})x_{24} + (-x_{44}x_{32} + x_{42}x_{34})x_{23} + (x_{44}x_{33} - x_{43}x_{34})x_{22},\\
&(x_{44}x_{33} - x_{43}x_{34})x_{25} + (-x_{45}x_{33} + x_{35}x_{43})x_{24} + (x_{45}x_{34} - x_{35}x_{44})x_{23})\\
&\subset \mathbb{Q}[x_{ij} \mid 1 \le i \le 4, 1 \le j \le 5].\\
A_{2,4,4} =&(-x_{21}x_{12} + x_{22}x_{11}, -x_{22}x_{13} + x_{23}x_{12}, -x_{23}x_{14} + x_{24}x_{13}, x_{32}x_{21} - x_{31}x_{22},\\
&x_{33}x_{22} - x_{32}x_{23}, x_{34}x_{23} - x_{24}x_{33}, x_{42}x_{31} - x_{41}x_{32}, x_{43}x_{32} - x_{42}x_{33},\\
&x_{44}x_{33} - x_{43}x_{34}) \subset \mathbb{Q}[x_{ij} \mid 1 \le i \le 4, 1 \le j \le 4].\\
A_{2,3,7} =&(-x_{21}x_{12} + x_{22}x_{11}, -x_{22}x_{13} + x_{23}x_{12}, -x_{23}x_{14} + x_{24}x_{13}, -x_{24}x_{15} + x_{25}x_{14},\\
&- x_{25}x_{16} + x_{26}x_{15}, -x_{26}x_{17} + x_{27}x_{16}, x_{32}x_{21} - x_{31}x_{22}, x_{33}x_{22} - x_{32}x_{23},\\
&x_{34}x_{23} - x_{24}x_{33}, x_{35}x_{24} - x_{25}x_{34}, x_{36}x_{25} - x_{26}x_{35}, x_{37}x_{26} - x_{36}x_{27})\\
&\subset \mathbb{Q}[x_{ij} \mid 1 \le i \le 3, 1 \le j \le 7].\\
T_1 =&(cdefghiz + cdefhjz + bcdeijz, 3cdfghz^3 + 4bdefghj + 4bdehjz^2,\\
&2bfghijz + fhjz^3, 4bcefhz + cfgijz, cdjz, 3egjz^4 + bcdgij + 2cdhjz^2,\\
&3defiz + 2defz^2 + 4bcei, 4bcefiz + 3dfhjz^2, cefhjz + bcfiz^2 + giz^4,\\
&4ceghiz + bcejz) \subset \mathbb{Q}[b, c, d, e, f, g, h, i, j, z].\\
T_2 =&(3bcegz^2 + 4bcghi + 2bcez^2, bcez + 3dhi, cfgiz^3 + bcdegh, cfgz^4 +\\
&3cdefgh, 2bcfgiz^2 + bcdegh + z^6, bchz + 4bcg, 4bcdgiz + 2cfhiz^2 +\\
&3bdfhi, bdefhz + bz^4, 3befgiz + 2cefgz^2 + 4cfhz^2, 3bfh + 4fhi + bz^2)\\
&\subset \mathbb{Q}[b, c, d, e, f, g, h, i, z].\\
T_3 =&(4befjkmz^3 + 2bcdhijlm + cdegkmz^2, cdeghjlz, 2defghilz + 4jlz^6 +\\
&defjlz^2, beghjlmz + 4ceghiz^2 + bdeflz^2) \subset \mathbb{Q}[b, c, d, e, f, g, h, i, j, k, l, m, z].\\
T_4 =&(2cfhiz^2 + bdefh, bcfijz + 4bcghi, 2cdejz + 4cdfj + ijz^2, bcdfgijz +\\
&cdijz^3, 3bceijz + 3cgijz^2 + beiz^3, 4bchjz + cgiz^2, behj, 3cdefhiz +\\
&2bdfgjz + 2bchjz^2) \subset \mathbb{Q}[b, c, d, e, f, g, h, i, j, z].\\
T_5 =&(4bc^2d^2e^2gh^2iz^2 + b^2ciz^9 + 2bceg^2hz^5, bcd^2e^2g^2h^2, bcfhz^5 + b^2dfg^2iz,\\
&4bc^2e^2f^2h^2i^2z^2 + b^2c^2e^2fh^2iz^3, 2b^2de^2f^2hi^2z + 3b^2c^2e^2h^2i^2)\\
&\subset \mathbb{Q}[b, c, d, e, f, g, h, i, z].\\
T_6 =&(4bcdfghlz + 3bcfhlz^3, befhkl + defghz, 3bdefhijklz + 2cfhjkz^5 +\\
&bdehkz^4, 4befijkl + dgklz^3, bcdefghj + 2bcdegijz + 2bcdhjklz,\\
&cdegijz + 3bcdefk + 4fhklz^2, 2bdeghjkz + cdez^5 + 3eghjz^3,\\
&bcdghijz + cdfhklz + 2bcdhkz^2, 2bcdefi + bhijkl, eghjkz^5 +\\
&2bcefghjkl, gilz^2 + 2beil, g, 3cdefijkl + 4bcdgjz^3, cdehijz + 4cegjz^3,\\
&bchkl, cdfghklz + befhilz + cdfgjlz, fiz^5 + 2cdfghk + bdfhiz,\\
&befijklz^2 + 3bcdghijl, 2bgijklz + 2bcghil + cefhjz, 2defghjz +
\end{aligned}
$$

$$
\begin{aligned}
&3cefhijz + 3bdghiz) \subset \mathbb{Q}[b,c,d,e,f,g,h,i,j,k,l,z].\\
T_7 =&(cfghijklz + cdz^7, 3bdikz^7 + 3bcdefghikl + 4bfghkz^5, 3befghijkz +\\
&2bcegijz^3, 3cfhjlz + dfhjlz + 4bdfkl, 3bejz^4 + bdfgjk + 2begjz^2,\\
&cdefgjkz + 3efgjlz^2 + 4elz^5, bcdefghjk, 4cehjlz^4 + 3ceghijkl,\\
&efghjklz, ik, 4beghijkz^3 + 3bdeghijkl, cdefkl + dgjklz, 2bghijlz +\\
&bcdgiz + 4eghjkz, bcehijklz + cdghijlz^2, 2bcdefglz + 2cfgijlz^2 +\\
&chz^6, 4bdefhjlz + bdhijlz + 2defgklz, 2cdgiklz + cehklz^2 + 4cghilz,\\
&chjkl, 2bcdhijlz + cgijz^4, bdfhijkz + 4bdijkz^3 + 2dhlz^4)\\
&\subset \mathbb{Q}[b,c,d,e,f,g,h,i,j,k,l,z].\\
T_8 =&(3bejz^4 + bdfgjk + 2begjz^2, cdefgjkz + 3efgjlz^2 + 4elz^5, bcdefghjk,\\
&4cehjlz^4 + 3ceghijkl) \subset \mathbb{Q}[b,c,d,e,f,g,h,i,j,k,l,z]\\
T_9 =&(3hz^4 + 2cdfg, bdefgh + cfgz^3 + cgz^4, bcgz^2 + cdef + defz, , 3efgh +\\
&bcez + 2bfz^2, 3defh + 2cegh, dehz + 4cgz^2, 2cdefhz + chz^3, 3cdefhz +\\
&2cfghz, 3dfghz + 2efhz^2 + 2bcgz, bdhz + 2efz + 2bhz)\\
&\subset \mathbb{Q}[b,c,d,e,f,g,h,z].\\
T_{10} =&(4cdfhjkz + 4efhijz^2 + cehiz^2, bcdfiz, 3bdefhj + 4cdeghz, cdegkz +\\
&bdiz^3, bcdkz^2 + 2begjk, 2cdefhijz + 3cehijz^3 + bcdhz^4, efhjkz + 3bcfhz,\\
&2bcegiz + 3dghijz + 3fghiz, bdfjz + dfjkz, 4efhikz + 3befhi + 2dfghi,\\
&cdhijz + 2efgkz^2, bcdgikz^2 + bcdfgik, dfgikz, 2bcdghiz + bcegiz^2 +\\
&bdfijk, cdefghijz, bcdegijkz + cdefkz^4, 4bdfghjz + bdgkz^3 + 2bcdeij,\\
&cefghijkz + 4defgikz^3 + 4eghkz^4, bcdgijkz + ceghjkz^2 + 4cefghz^3)\\
&\subset \mathbb{Q}[b,c,d,e,f,g,h,i,j,k,z].\\
P_1 =&(x) \subset \mathbb{Q}[x,y,z].\\
P_2 =&(x_{13}, x_{23}, x_{33}, x_{43}) \subset \mathbb{Q}[x_{ij} \mid 1 \le i \le 4, 1 \le j \le 5].\\
P_3 =&(b,z) \subset \mathbb{Q}[b,c,d,e,f,g,h,i,j,z].\\
P_4 =&(e,i,z) \subset \mathbb{Q}[b,c,d,e,f,g,h,i,j,z].\\
P_5 =&(g,h,z) \subset \mathbb{Q}[b,c,d,e,f,g,h,i,z].\\
P_6 =&(h,z) \subset \mathbb{Q}[b,c,d,e,f,g,h,i,j,k,l,m,z].\\
P_7 =&(b,j,z) \subset \mathbb{Q}[b,c,d,e,f,g,h,i,j,z].\\
P_8 =&(f,g,i) \subset \mathbb{Q}[b,c,d,e,f,g,h,i,z].\\
P_9 =&(z^4 + hdb, c, g, k, l) \subset \mathbb{Q}[b,c,d,e,f,g,h,i,j,k,l,z].\\
P_{10} =&(b,c,e,h,i,j) \subset \mathbb{Q}[b,c,d,e,f,g,h,i,j,k,l,z].\\
P_{11} =&(e,k) \subset \mathbb{Q}[b,c,d,e,f,g,h,i,j,k,l,z].\\
P_{12} =&(e,g,z) \subset \mathbb{Q}[b,c,d,e,f,g,h,z].\\
P_{13} =&(e,g,k,z) \subset \mathbb{Q}[b,c,d,e,f,g,h,i,j,k,z].\\
P_{14} =&(x,y) \subset \mathbb{Q}[x,y,z].\\
P_{15} =&(x_{12}x_{31} - x_{32}x_{11}, x_{42}x_{11} - x_{41}x_{12}, x_{42}x_{31} - x_{41}x_{32}, x_{44}x_{31} - x_{41}x_{34},\\
&x_{44}x_{32} - x_{42}x_{34}, x_{13}, x_{21}, x_{22}, x_{23}, x_{24}, x_{33}, x_{43})\\
&\subset \mathbb{Q}[x_{ij} \mid 1 \le i \le 4, 1 \le j \le 4].\\
P_{16} =&(x_{16}x_{27} - x_{17}x_{26}, x_{34}x_{13} - x_{33}x_{14}, x_{37}x_{16} - x_{36}x_{17}, x_{36}x_{27} - x_{37}x_{26},
\end{aligned}
$$

$$x_{12}, x_{15}, x_{21}, x_{22}, x_{23}, x_{24}, x_{25}, x_{32}, x_{35}) \subset \mathbb{Q}[x_{ij} \mid 1 \leq i \leq 3, 1 \leq j \leq 7].$$

$$P_{17} = (e, f, j, z) \subset \mathbb{Q}[b, c, d, e, f, g, h, i, j, z].$$

$$P_{18} = (c, d, j, z) \subset \mathbb{Q}[b, c, d, e, f, g, h, i, j, z].$$

$$P_{19} = (-4fec + 3d, b, g, h, z) \subset \mathbb{Q}[b, c, d, e, f, g, h, i, z].$$

$$P_{20} = (lfdb + 4higc, e, j, m) \subset \mathbb{Q}[b, c, d, e, f, g, h, i, j, k, l, m, z].$$

$$P_{21} = (c, d, h, j, z) \subset \mathbb{Q}[b, c, d, e, f, g, h, i, j, z].$$

$$P_{22} = (c, d, g, i, z) \subset \mathbb{Q}[b, c, d, e, f, g, h, i, z].$$

$$P_{23} = (b, c, d, e, f, g, h, i, z) \subset \mathbb{Q}[b, c, d, e, f, g, h, i, j, k, l, z].$$

$$P_{24} = (g, i, j, l, z) \subset \mathbb{Q}[b, c, d, e, f, g, h, i, j, k, l, z].$$

$$P_{25} = (f, g, k, z) \subset \mathbb{Q}[b, c, d, e, f, g, h, i, j, k, l, z].$$

$$P_{26} = (c, e, g, h, z) \subset \mathbb{Q}[b, c, d, e, f, g, h, z].$$

$$P_{27} = (c + 4jf, b, d, g, h, k, z) \subset \mathbb{Q}[b, c, d, e, f, g, h, i, j, k, z].$$

Communications of JSSAC (2020)
Vol. 4, pp. 33 – 49

Simple Signature-Based Algorithms with Correctness and Termination

Kosuke Sakata*

Graduate School of Environment and Information Sciences, Yokohama National University

(Received 3/Jun/2020 Accepted 12/Nov/2020)

Abstract

We show correctness and termination of signature-based algorithms for computing Gröbner bases, together with some remarks on those algorithms. Compared to rewrite basis algorithm introduced by Eder and Roune in 2012, we describe an equivalent algorithm called "alternative rewrite basis algorithm" more concretely, with giving self-contained proofs of the correctness and the termination of the algorithm more clearly and transparently. The original rewrite basis algorithm seems to be designed so that it is efficient when POT is chosen as a module order and it proceeds incrementally like: computing Gröbner bases of $\langle f_1 \rangle$, $\langle f_1, f_2 \rangle$, $\langle f_1, f_2, f_3 \rangle, \ldots, \langle f_1, f_2, \ldots, f_m \rangle$ in order for polynomials $\{f_i\}_{i=1,2,3,\ldots,m}$. We clarify the reason of the efficiency in that case. If we use the original rewrite basis algorithm with a module order other than POT, we compute extra zero reductions. The algorithm presented in this paper is modified to keep the efficiency as much as possible when we choose a module order other than POT.

Keywords: Gröbner Basis, rewrite basis algorithm, signature-based algorithm

1 Introduction

Gröbner bases are one of important research topics in algebra and is widely used in applications. It is well-known that Gröbner bases are utilized for solving systems of polynomial equations. In cryptography, Gröbner basis method was utilized for breaking a challenge of the first hidden field equations (HFE) crypto system [10]. For other applications like coding theory, statistics and integer programming problem etc., it is possible to obtain a solution by converting a problem into a polynomial system and computing its Gröbner basis. Some engineering problems are necessary to be dealt with problems of polynomial systems including parameters. For these problems, there exits algorithms for computing comprehensive Gröbner bases. In the algorithms, Gröbner bases are computed multiple times. In summary, Gröbner bases have a wide range of applications. It can be expected that many works for such applications would progress by improving Gröbner basis algorithms, as it accelerates computation of Gröbner bases.

*sakata-kosuke-rb@g.ecc.u-tokyo.ac.jp

In 1964, Buchberger [2] introduced the notion of Gröbner bases and proposed an algorithm for computing Gröbner bases. Since then, various improvements about the algorithm have been proposed. As for computing a Gröbner basis, it is required to simplify polynomials, called a reduction. Elements of a Gröbner basis are generated by reducing polynomials, and some polynomials are reduced to zero. The computations of zero reductions do not give any information of the Gröbner basis. Moreover the number of zero reductions is tend to be larger than that of nonzero reductions. Therefore, in order to decrease amount of calculations, methods for detecting polynomials which are reduced to zero have been studied by many researchers.

One important improvement of Gröbner basis algorithms is F5 algorithm proposed by Faugère in 2002 [9]. F5 algorithm discards many polynomials that are reduced to zero, comparing to conventional algorithms.

When first proposed, the algorithm was complicated and the proof was incomplete. Since then, F5 has been deeply studied and accurate proofs of correctness and termination have been submitted (main references are [5, 11, 12, 14, 15]). Several algorithms and methods for improving F5 have been proposed (main references are [1, 3, 4, 6, 8, 13]). F5 is now recognized as one of signature-based algorithms. The paper [7] compiled studies of signature-based algorithms, so that we can overview research of signature-based algorithms. In the paper, signature-based algorithms are generalized as rewrite basis algorithm (**RB**) [6]. The algorithm in [1] called Arri and the algorithm in [13] called GVW are introduced as **RB** with RAT selected for a rewrite order. The explanations and the definitions of rewrite basis algorithm, a rewrite order and RAT are not given in this paper because they are too long. When we choose RAT for a rewrite order, rewrite basis algorithm becomes the most efficient. The proofs of correctness and termination in [7] are not self-contained unfortunately. Additionally, **RB** is not provided as an efficient algorithm in case we choose module orders other than POT (position over term) because **RB** is introduced as a generalized signature-based algorithm.

In this paper, we introduce alternative rewrite basis algorithm (**altRB**) (see **Algorithm 4** in Section 6). This algorithm is efficient for an arbitrary module order other than POT, and moreover it is concrete enough to be implemented. As the main results of this paper, we prove the correctness (Theorem 20) and the termination (Theorem 21) of **altRB**. By designing the algorithm concretely, the proofs of the correctness and the termination are clearer and more transparent. The proofs are done by several steps. In each step, we discuss the correctness and the termination of an algorithm. The algorithms are fundamental signature-based semi-algorithm[1)] (**fundSB**), simple signature-based algorithm (**simpleSB**), simple syzygy signature-based algorithm (**syzSB**), alternative rewrite basis algorithm (**altRB**). The algorithms in earlier steps are less complex. We believe that the proofs of Theorem 20 and Theorem 21 are easy for the reader to understand, as so are the proofs of each step. In Section 7, we prove that RB has an exceptional advantage when POT is chosen for a module order and RB proceeds incrementally. On the other hand, **altRB** is designed to be suitable for an arbitrary module order.

This paper is organized as follows. In Section 2, we recall notations and definitions in [7] of signature-based algorithms. In Section 3, we focus on that signature-based algorithms compute a Gröbner basis in the ascending order of signature. In order to look at the behavior of the algorithms, we study fundamental signature-based semi-algorithm (**fundSB**), which is simpler than subsequent algorithms. Although this semi-algorithm does not terminate, it helps us grasp the idea and how signature-based algorithms work, and also make clear the proofs of the correctness and the termination of the subsequent algorithms. In Section 4, we study a basic signature-based algorithm, which terminates in finite steps. The algorithm is called "simple signature-based algorithm (**simpleSB**)".

[1)] When the word semi-algorithm is used, it is intended that the process may not terminate. The word semi-algorithm is used only for fundamental signature-based semi-algorithm (**fundSB**).

It is essentially equivalent to the algorithm genSB [7]. However, the proofs of the correctness and the termination are partially different to those of [7] and are described in detail. In Section 5, we focus on methods for detecting polynomials which are reduced to zero. The methods are specific to signature-based algorithms. Simple syzygy signature-based algorithm (**syzSB**) is considered to illustrate the method. In Section 6, alternative rewrite basis algorithm (**altRB**) is introduced. We show the termination and the correctness of **altRB**. In Section 7, we discuss the number of zero reductions and module orders as in one previous paragraph.

It is known that signature-based algorithms compute not only a signature Gröbner basis but also a Gröbner basis of the syzygy module for a given input system. **syzSB** and **altRB** outputs the leading terms of Gröbner basis of the syzygy module. If you give small modification, they can output a Gröbner basis itself. But we do not refer to the fact and its proofs, see [13] and [7].

2 Notation

Let R be a polynomial ring over a field K. Let us denote $K \setminus \{0\}$ by $K^\times$. For $a, b \in R$, we write $a \mid b$ if b is divisible by a.

Let $f_1, f_2, \ldots, f_m$ be elements of R. Let $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_m$ be the standard basis of a free module R^m. Consider the homomorphism

$$\overline{\ }: \quad R^m \quad \longrightarrow \quad R$$

defined by

$$\alpha = \sum_{i=1}^{m} a_i \mathbf{e}_i \quad \longmapsto \quad \overline{\alpha} = \sum_{i=1}^{m} a_i f_i,$$

where $a_1, \ldots, a_m \in R$, especially $\overline{\mathbf{e}_i} = f_i$ holds.

We choose a monomial order $\leq$ on R, and choose a module order $\preceq$. The module order is required to be compatible with the monomial order, that means: $a\mathbf{e}_i \preceq b\mathbf{e}_i$ for $i = 1, \ldots, m$ for all monomials $a, b \in R$ in case $a \leq b$. An element of R^m of the form $a\mathbf{e}_i$ for a monomial a of R is called a *term* of R^m. Let $\alpha = a\mathbf{e}_i$ and $\beta = b\mathbf{e}_j$ be terms, if there exists $c \in K^\times$ such that $a = cb$ and $i = j$, we write $\alpha \simeq \beta$ and we say that α and β are *equivalent*. If $a \mid b$ and $i = j$, we write $\alpha \mid \beta$. For $f \in R$, $\mathrm{LT}(f)$ denotes the leading term of f with respect to the monomial order. For $\alpha \in R^m$, the *signature* $\mathfrak{s}(\alpha)$ of α is defined to be the leading term of α with respect to the module order.

Let G be a subset of R^m. For $\alpha, \alpha' \in R^m$, we say that α is $\mathfrak{s}$-*reduced* to α' if there exist $\beta \in G$ and $b \in R$ satisfying the three conditions:

(a) $\mathrm{LT}(\overline{b\beta}) = t$ for a (certain) monomial t in $\overline{\alpha}$

(b) $\mathfrak{s}(b\beta) \preceq \mathfrak{s}(\alpha)$

(c) $\alpha' = \alpha - b\beta$.

At this time, we call β a reducer. We say that α is *singularly* $\mathfrak{s}$-*reduced* to α' if the condition **(b)** above is replaced by $\mathfrak{s}(b\beta) \simeq \mathfrak{s}(\alpha)$, and otherwise that α is *regularly* $\mathfrak{s}$-*reduced* to α'. If there exists $c \in K$ such that $\mathrm{LT}(\overline{b\beta}) = c\,\mathrm{LT}(\overline{\alpha})$, the $\mathfrak{s}$-reduction is called *top* $\mathfrak{s}$-*reduction* and otherwise called *tail* $\mathfrak{s}$-*reduction*. If the $\alpha \in R^m$ cannot be $\mathfrak{s}$-reduced, we say that α is *completely* $\mathfrak{s}$-*reduced*. If the $\alpha \in R^m$ cannot be regularly top $\mathfrak{s}$-reduced, we say that α is *completely regularly top* $\mathfrak{s}$-*reduced*. If the $\alpha \in R^m$ can be both neither regularly top $\mathfrak{s}$-reduced nor regularly tail $\mathfrak{s}$-reduced, we say that α is *completely regularly full* $\mathfrak{s}$-*reduced*. If $\alpha \in R^m$ is completely $\mathfrak{s}$-reduced and $\overline{\alpha}$ is $0 \in R$, then we say

that α is completely $\mathfrak{s}$-reduced to $0 \in R$ (Remark: it does not mean that α is completely $\mathfrak{s}$-reduced to $0 \in R^m$).

A subset $G \subseteq R^m$ is *a signature Gröbner basis up to signature T* if all $\alpha \in R^m$ with $\mathfrak{s}(\alpha) \prec T$ are completely $\mathfrak{s}$-reduced to $0 \in R$ with respect to G. A subset $G \subseteq R^m$ is *a signature Gröbner basis in signature T* if all $\alpha \in R^m$ with $\mathfrak{s}(\alpha) \prec T$ are completely $\mathfrak{s}$-reduced to $0 \in R$ with respect to G. A subset $G \subseteq R^m$ is *a signature Gröbner basis* if all $\alpha \in R^m$ are $\mathfrak{s}$-reduced to $0 \in R$ with respect to G. The signature-based algorithms compute a signature Gröbner basis. If G is a signature Gröbner basis, then $\{\overline{g} \mid g \in G\}$ is a Gröbner basis of the ideal generated by $\{\overline{g} \mid g \in G\}$.

Proposition 1
Let I be the ideal generated by $\{f_1, \ldots, f_m\}$, let G be a signature Gröbner basis. Then, $\{\overline{g} \mid g \in G\}$ is a Gröbner basis of the ideal $\langle \overline{g} \mid g \in G \rangle$.

Proof First, we show $\overline{\alpha} \in I$ for any $\alpha \in G$. Let $\alpha \in G$, which is written as $\sum_{i=1}^{m} r_i \mathbf{e}_i$, for $r_i \in R$. Then $\overline{\alpha} = \sum_{i=1}^{m} r_i \overline{\mathbf{e}_i} = \sum_{i=1}^{m} r_i f_i$.

Assume that $\{\overline{g} \mid g \in G\}$ is not a Gröbner basis of I. Then, there exists $h \in I$ such that h is not top reducible by $\{\overline{g} \mid g \in G\}$. As $h \in I$, one can write h as $\sum_{i=1}^{m} a_i f_i$ for $a_i \in R$. Put $\beta = \sum_{i=1}^{m} a_i \mathbf{e}_i \in R^m$. Then, we have $\overline{\beta} = h$. Since G is a signature Gröbner basis, β is top $\mathfrak{s}$-reducible. This means that h is top reducible. This is a contradiction. ∎

A signature Gröbner basis G is *minimal* if there does not exist an element α in G which top $\mathfrak{s}$-reduces any other elements in $G \setminus \{\alpha\}$. We also use the word "minimal" for a signature Gröbner basis in G and up to G.

3 Fundamental signature-based semi-algorithm

In this section, fundamental signature-based semi-algorithm (**fundSB**) is considered. It helps us to comprehend how signature-based algorithms work. Specifically almost all signature-based algorithms proceed in the ascending order of signatures. **fundSB** is a prototype of them. **Algorithm 1** is the pseudocode of **fundSB**.

Algorithm 1 Fundamental signature-based semi-algorithm (**fundSB**)

Input : a finite subset $F = \{f_1, \ldots, f_m\}$ of R.

Step 1 $\alpha \leftarrow$ the minimal term in R^m which is bigger than the terms computed before
Step 2 $\alpha' \leftarrow$ result of completely regularly top $\mathfrak{s}$-reducing α by G
Step 3 (i) If $\overline{\alpha'} = 0$
Go to Step 1
(ii) If $\overline{\alpha'} \neq 0$
(a) If α' is singularly top $\mathfrak{s}$-reducible by G
Go to Step 1
(b) If α' is not singularly top $\mathfrak{s}$-reducible by G
$G \leftarrow G \cup \{\alpha'\}$
Go to Step 1

fundSB does not terminate, because it will compute all terms in R^m and the number of elements of R^m are infinite. However, we can prove the following properties:

(A) at the end of Step 3, G is a signature Gröbner basis in α,

(B) at the end of Step 1, G is a signature Gröbner basis up to α.

If **(A)** is satisfied, **(B)** is true because **fundSB** computes in the ascending order of terms in R^m step by step. We shall prove **(A)** in Proposition 5. For this, we need Lemmas 2, 3 and 4 below.

Remark : fundSB could terminate, if we modify **fundSB** as following:

(1) Select a term $\beta \in R^m$, a monomial order and a module order such that the number of terms up to β is finite.

(2) Terminate **fundSB** when the calculation progresses to β.

In this case, **fundSB** outputs a signature Gröbner basis up to β.

Lemma 2 is called singular criterion [3].

Lemma 2
Let T be a term in R^m and let G be a signature Gröbner basis up to T. Let α and β in R^m satisfy

(1) $\mathfrak{s}(\alpha) = \mathfrak{s}(\beta) \preceq T$,

(2) α *and* β *are completely regularly top* $\mathfrak{s}$*-reduced by* G.

Then, $\mathrm{LT}(\overline{\alpha}) = \mathrm{LT}(\overline{\beta})$. *Moreover, if* α *and* β *are completely regularly* $\mathfrak{s}$*-reduced, then* $\overline{\alpha} = \overline{\beta}$.

Proof (The former) Assume that $\mathrm{LT}(\overline{\alpha}) \neq \mathrm{LT}(\overline{\beta})$. Then, either $\mathrm{LT}(\overline{\alpha-\beta}) = \mathrm{LT}(\overline{\alpha})$ or $\mathrm{LT}(\overline{\alpha-\beta}) = \mathrm{LT}(\beta)$ is satisfied. Since $\mathfrak{s}(\alpha) = \mathfrak{s}(\beta)$, we have $\mathfrak{s}(\alpha-\beta) \prec \mathfrak{s}(\alpha) \preceq T$. Therefore, $\alpha-\beta$ is top $\mathfrak{s}$-reducible by G, that is, there exists a pair $(\gamma, a) \in G \times R$ such that $\mathfrak{s}(a\gamma) \preceq \mathfrak{s}(\alpha-\beta)$ and $\mathrm{LT}(\overline{a\gamma}) = \mathrm{LT}(\overline{\alpha-\beta})$. This $a\gamma$ satisfies that $\mathfrak{s}(a\gamma) \prec \mathfrak{s}(\alpha) = \mathfrak{s}(\beta)$ and either $\mathrm{LT}(\overline{a\gamma}) = \mathrm{LT}(\overline{\alpha})$ or $\mathrm{LT}(\overline{a\gamma}) = \mathrm{LT}(\overline{\beta})$. Then, $a\gamma$ regularly top $\mathfrak{s}$-reduce α or β. This contradicts that α and β are completely regularly top $\mathfrak{s}$-reduced.

(The latter) Assume that $\overline{\alpha-\beta} \neq 0$. The leading term of $\overline{\alpha-\beta}$ is the term included in either $\overline{\alpha}$ or $\overline{\beta}$. Since $\mathfrak{s}(\alpha) = \mathfrak{s}(\beta)$, we have $\mathfrak{s}(\alpha-\beta) \prec \mathfrak{s}(\alpha) \preceq T$. Therefore, $\alpha-\beta$ is top $\mathfrak{s}$-reducible by G, that is, there exists a pair$(\gamma, a) \in (G, R)$ such that $\mathfrak{s}(a\gamma) \preceq \mathfrak{s}(\alpha-\beta)$ and $\mathrm{LT}(\overline{a\gamma}) = \mathrm{LT}(\overline{\alpha-\beta})$. This $a\gamma$ satisfies that $\mathfrak{s}(a\gamma) \prec \mathfrak{s}(\alpha) = \mathfrak{s}(\beta)$ and there exists a term in $\overline{\alpha}$ or $\overline{\beta}$ such that the term is the same as $\mathrm{LT}(\overline{a\gamma})$. Then, $a\gamma$ regularly $\mathfrak{s}$-reduce α or β. This contradicts that α and β are completely regularly $\mathfrak{s}$-reduced. ∎

Let T be a term in R^m. When we have a signature Gröbner basis up to $T \in R^m$, and let $\alpha \in R^m$ satisfy $\mathfrak{s}(\alpha) \preceq T$ and α is completely regularly top $\mathfrak{s}$-reduced and singularly top $\mathfrak{s}$-reducible, then we can discard α thanks to Lemmas 3 and 4 below.

Lemma 3
Let T be a term in R^m and let G be a signature Gröbner basis up to T. Let $\alpha \in R^m$ and $\beta \in G$ satisfy

(1) $\mathfrak{s}(\alpha) \preceq T$,

(2) α *is completely regularly top* $\mathfrak{s}$*-reduced by* G,

(3) there exists $a \in R$ *which satisfies* $\mathfrak{s}(\alpha) \simeq \mathfrak{s}(a\beta)$ *and* $\mathrm{LT}(\overline{\alpha}) = \mathrm{LT}(\overline{a\beta})$.

Then, $\mathfrak{s}(\alpha) = \mathfrak{s}(a\beta)$.

Proof Assume that $\mathfrak{s}(\alpha) \neq \mathfrak{s}(a\beta)$. Then, there exists $c \in K$ that satisfies $c \neq 1$ and $\mathfrak{s}(\alpha) = c\mathfrak{s}(a\beta)$. Since $\mathfrak{s}(\alpha - ca\beta) \prec \mathfrak{s}(\alpha) \preceq T$, we have that $\alpha - ca\beta$ is top $\mathfrak{s}$-reducible by G. Therefore, there exists a pair $(\gamma, b) \in G \times R$ that satisfies $\mathfrak{s}(b\gamma) \preceq \mathfrak{s}(\alpha - ca\beta)$ and $\mathrm{LT}(\overline{b\gamma}) = \mathrm{LT}(\overline{\alpha - ca\beta})$. Since $\mathrm{LT}(\overline{\alpha - ca\beta}) \simeq \mathrm{LT}(\overline{\alpha})$, we have that γ regularly top $\mathfrak{s}$-reduce α. This contradicts that α is completely regularly top $\mathfrak{s}$-reduced. ∎

Lemma 4
Let T be a term in R^m and let G be a signature Gröbner basis up to T. Let $\alpha \in R^m$ satisfies

(1) $\mathfrak{s}(\alpha) \preceq T$,

(2) α is completely regularly top $\mathfrak{s}$-reduced by G,

(3) α is singular top $\mathfrak{s}$-reducible by G.

Then, α is $\mathfrak{s}$-reduced to $0 \in R$ by G.

Proof Let $\beta \in G$ be a reducer which singularly top $\mathfrak{s}$-reduces α. From Lemma 3, there exists $a \in R$ that satisfies $\mathrm{LT}(\overline{\alpha}) = \mathrm{LT}(\overline{a\beta})$ and $\mathfrak{s}(\alpha) = \mathfrak{s}(a\beta)$. Then, we have that $\mathfrak{s}(\alpha - a\beta) \prec \mathfrak{s}(\alpha)$, so $\alpha - a\beta$ is $\mathfrak{s}$-reduced to $0 \in R$ by G. ∎

Let us prove **(A)** mentioned in the second paragraph of this section.

Proposition 5
At the end of Step 3 in **fundSB**, *G is a signature Gröbner basis in α at the every loop.*

Proof Let α be the term chosen in the latest Step 1. Let α' be the result of completely regularly top $\mathfrak{s}$-reducing α. Let G be a signature Gröbner basis up to α. We prove that G is a signature Gröbner basis in α after the end of Step 3, that is, all $\beta \in R^m$ with $\mathfrak{s}(\beta) \preceq \alpha$ are $\mathfrak{s}$-reduced to $0 \in R$ by G.

Since G is a signature Gröbner basis up to α, then $\beta \in R^m$ with $\mathfrak{s}(\beta) \prec \alpha$ is $\mathfrak{s}$-reduced to $0 \in R$ by G. Then, let β satisfy $\mathfrak{s}(\beta) \simeq \alpha$. As we $\mathfrak{s}$-reduce β by G step by step, suppose β would be changed as follows: $\beta \to \beta^{(1)} \to \beta^{(2)} \to \cdots \to \beta^{(i)} \to \cdots$. Assume an $\mathfrak{s}$-reduction such that $\mathfrak{s}(\beta^{(i)}) = \mathfrak{s}(a\gamma)$ $(a \in R, \gamma \in G)$ occurs for a certain i. Since $\mathfrak{s}(\beta^{(i+1)}) \prec \alpha$ for the i, in this case, β is $\mathfrak{s}$-reduced to $0 \in R$. Suppose that such an $\mathfrak{s}$-reduction does not occur. Let β' be the result of completely $\mathfrak{s}$-reducing β. Note that $\mathfrak{s}(\beta') \simeq \alpha$ and β' is completely regularly top $\mathfrak{s}$-reduced. From Lemmas 2 and 3, there exists $c \in K$ such that $\mathfrak{s}(\alpha') = c\mathfrak{s}(\beta')$ and $\mathrm{LT}(\overline{\alpha'}) = c\,\mathrm{LT}(\overline{\beta'})$.

We consider the result of $\mathfrak{s}$-reducing β in the following three cases according to how α' was handled in Step 3.

(i) If $\overline{\alpha'} = 0$, then β' as well as α' is $\mathfrak{s}$-reduced to $0 \in R$ by Lemma 2.

(ii) If $\overline{\alpha'} \neq 0$ and α' is singularly top $\mathfrak{s}$-reducible, then β' as well as α' is singularly top $\mathfrak{s}$-reducible. By Lemma 4, we have that β' is $\mathfrak{s}$-reduced to $0 \in R$.

(iii) If $\overline{\alpha'} \neq 0$ and α' is not singularly top $\mathfrak{s}$-reducible, then β' is singularly top $\mathfrak{s}$-reducible by α' since $\mathfrak{s}(\alpha') = c\mathfrak{s}(\beta')$ and $\mathrm{LT}(\overline{\alpha'}) = c\,\mathrm{LT}(\overline{\beta'})$, and α' is included in G. By Lemma 4, β' is $\mathfrak{s}$-reduced to $0 \in R$.

From the above, we have proved that all $\beta \in R^m$ with $\mathfrak{s}(\beta) \preceq \alpha$ are $\mathfrak{s}$-reduced to $0 \in R$ by G. Thus, G is a signature Gröbner basis in α at the end of Step 3. ∎

The set G computed in **fundSB** is minimal.

Lemma 6
Let $T \in R^m$ be a term chosen at Step 1 in **fundSB**. *Let G in* **fundSB** *be the set after Step3 of T. Then, G is a minimal signature Gröbner basis in T.*

Proof By Proposition 5, G is a signature Gröbner basis in T. Let α be an element in G. For $\beta \in G$ with $\mathfrak{s}(\beta) \prec \mathfrak{s}(\alpha)$, clearly β is not top $\mathfrak{s}$-reducible by α. For $\beta \in G$ with $\mathfrak{s}(\beta) \succeq \mathfrak{s}(\alpha)$, β is not regularly top $\mathfrak{s}$-reducible by α because of Step 2. Moreover, β is not singularly top $\mathfrak{s}$-reducible by α because of Step 3 (ii) (b). Then, β is not top $\mathfrak{s}$-reducible by α. Thus, there is no element in G which top $\mathfrak{s}$-reduces any other elements in G. Therefore, G is a minimal signature Gröbner basis in T. ∎

4 Simple signature-based algorithm

In this section, we introduce simple signature-based algorithm (**simpleSB**), and show that it terminates and outputs a signature Gröbner basis. Before introducing the algorithm, we define an S-pair, which is an analogy of S-polynomial. The *S-pair* of $\alpha, \beta \in R^m$ is defined to be

$$\mathrm{spair}(\alpha,\beta) = \frac{\lambda}{\mathrm{LT}(\overline{\alpha})}\alpha - \frac{\lambda}{\mathrm{LT}(\overline{\beta})}\beta,$$

where λ is the least common multiple (of monomials) as $\lambda = \mathrm{lcm}(\mathrm{LT}(\overline{\alpha}), \mathrm{LT}(\overline{\beta}))$. If

$$\mathfrak{s}\left(\frac{\lambda}{\mathrm{LT}(\overline{\alpha})}\alpha\right) \simeq \mathfrak{s}\left(\frac{\lambda}{\mathrm{LT}(\overline{\beta})}\beta\right),$$

we say that the S-pair is *singular*, otherwise, we say that the S-pair *regular*. **Algorithm 2** is the pseudocode of **simpleSB**. Note that **simpleSB** outputs a minimal signature Gröbner basis by Lemma 6.

Algorithm 2 Simple signature-based algorithm (**simpleSB**)

Input : a finite subset $F = \{f_1, \ldots, f_m\}$ of R.
Output: a minimal signature Gröbner basis G of F.

Step 0 $G \leftarrow \emptyset, P \leftarrow \{\mathbf{e}_1, \ldots, \mathbf{e}_m\}$
Step 1 If $P = \emptyset$, return G
$\alpha \leftarrow$ the minimal term in P
$P \leftarrow P \backslash \{\alpha\}$
Step 2 $\alpha' \leftarrow$ result of completely regularly top $\mathfrak{s}$-reducing α by G
Step 3 (i) If $\overline{\alpha'} = 0$
Go to Step 1
(ii) If $\overline{\alpha'} \neq 0$
(a) If α' is singularly top $\mathfrak{s}$-reducible by G
Go to Step 1
(b) If α' is not singularly top $\mathfrak{s}$-reducible by G
$P \leftarrow P \cup \{\mathfrak{s}(\mathrm{spair}(\alpha', \beta)) \mid \beta \in G, \mathrm{spair}(\alpha', \beta) \text{ is regular}\}$ (#)
$G \leftarrow G \cup \{\alpha'\}$
Go to Step 1

Remark : In Step 2 of Algorithm 2, we execute only regularly "top" $\mathfrak{s}$-reduction depending on the description of the algorithm. However, we can execute regularly "tail" $\mathfrak{s}$-reduction, and the correctness and the termination of the algorithm are not affected by the modification. In terms of (#) in **simpleSB**, it is sufficient to leave only one term α among terms which are equivalent to α in P. Even if more than two equivalent terms are left in P, **simpleSB** terminates and outputs a signature Gröbner basis.

Let us give an outline of the proofs of the correctness and the termination. The difference between **fundSB** and **simpleSB** is that **simpleSB** computes terms in R^m that appear in Step 3 (ii) (b). In Proposition 12, we prove that G is a signature Gröbner basis in α when Step 3 for α is finished. It follows from Lemma 11 that it is not necessary to compute terms $\preceq \alpha$ that do not appear at (#). The termination of **simpleSB** is proved by Proposition 13. When the algorithm terminates, G is a signature Gröbner basis, by Lemma 11 and Propositions 14 and 12.

Lemmas 7, 8, 9 and 10 are used for proving Lemma 11.

Lemma 7
Let T be a term in R^m and let G be a signature Gröbner basis up to T. Let $\alpha \in G$ and let a be a monomial in R satisfy

(1) $\mathfrak{s}(a\alpha) \preceq T$,

(2) $a\alpha$ *is regularly top* $\mathfrak{s}$*-reducible by* G.

Then, there exists an S-pair $a'\alpha - b\beta$ (a' and b are monomials in R, β is in G) such that

(3) $\mathfrak{s}(a'\alpha - b\beta) = \mathfrak{s}(a'\alpha)$,

(4) $a' \mid a$.

Proof Let a' be the minimal monomial in the set consisting of the monomials $r \in R$ satisfying that $r \mid a$ and $r\alpha$ is regularly top $\mathfrak{s}$-reducible. Since $a'\alpha$ is regularly top $\mathfrak{s}$-reducible, there exists a pair $(\beta, b) \in G \times R$ such that $\mathfrak{s}(a'\alpha) \succ \mathfrak{s}(b\beta)$ and $\mathrm{LT}(\overline{a'\alpha}) = \mathrm{LT}(\overline{b\beta})$. Let $d = a' \mathrm{LT}(\overline{\alpha}) = b \mathrm{LT}(\overline{\beta})$. Assume that $\mathrm{GCD}(a', b) = m$ with $m \neq 1$. Then, a' and b are written as $a' = ma''$ and $b = mb'$ such that $\mathrm{GCD}(a'', b') = 1$. For $a''\alpha$ and $b'\beta$, note that $\mathfrak{s}(a'\alpha) \succ \mathfrak{s}(b\beta)$ leads to $\mathfrak{s}(a''\alpha) \succ \mathfrak{s}(b'\beta)$ and $a' \mathrm{LT}(\overline{\alpha}) = b \mathrm{LT}(\overline{\beta})$ leads to $a'' \mathrm{LT}(\overline{\alpha}) = b' \mathrm{LT}(\overline{\beta})$. This means that $a''\alpha$ is regularly top $\mathfrak{s}$-reducible and $a'' < a'$. This contradicts the minimality of a'. Therefore, $m = 1$ and $\mathrm{GCD}(a', b) = 1$. There exists $e \in K^\times$ such that $d = e \,\mathrm{lcm}(\mathrm{LT}(\overline{\alpha}), \mathrm{LT}(\overline{\beta}))$. Then, we have

$$a'\alpha - b\beta = \frac{d}{\mathrm{LT}(\overline{\alpha})}\alpha - \frac{d}{\mathrm{LT}(\overline{\beta})}\beta = \frac{e \,\mathrm{lcm}(\mathrm{LT}(\overline{\alpha}), \mathrm{LT}(\overline{\beta}))}{\mathrm{LT}(\overline{\alpha})}\alpha - \frac{e \,\mathrm{lcm}(\mathrm{LT}(\overline{\alpha}), \mathrm{LT}(\overline{\beta}))}{\mathrm{LT}(\overline{\beta})}\beta.$$

This is an S-pair satisfying (3) and (4). ∎

Lemma 8
Let T be a term in R^m and let G be a signature Gröbner basis up to T. Let $\alpha \in R^m$ satisfy

(1) $\mathfrak{s}(\alpha) \preceq T$,

(2) α *is completely regularly top* $\mathfrak{s}$*-reduced by* G.

Then, any pair $(\beta, a) \in G \times R$ with $\mathfrak{s}(\alpha) = \mathfrak{s}(a\beta)$ satisfies $\mathrm{LT}(\overline{\alpha}) \leq \mathrm{LT}(\overline{a\beta})$.

Proof Assume that there exists a pair $(\beta, a) \in G \times R$ such that $\mathfrak{s}(\alpha) = \mathfrak{s}(a\beta)$ and $\mathrm{LT}(\overline{\alpha}) > \mathrm{LT}(\overline{a\beta})$. Let γ be the result of completely regularly top $\mathfrak{s}$-reducing $a\beta$. Then, we have $\mathrm{LT}(\overline{\alpha}) > \mathrm{LT}(\overline{a\beta}) \geq \mathrm{LT}(\overline{\gamma})$ and $\mathfrak{s}(\alpha) = \mathfrak{s}(\gamma)$. This contradicts Lemma 2. ∎

Lemma 9
Let T be a term in R^m and let G be a signature Gröbner basis up to T. Let $\alpha \in G$ and let a be a monomial in R satisfy

(1) $\mathfrak{s}(a\alpha) \preceq T$,

(2) $a\alpha$ *is completely regularly top* $\mathfrak{s}$*-reduced by* G.

Then, there do not exists a pair $(\beta, b) \in G \times R$ such that

(3) $\mathfrak{s}(a\alpha - b\beta) = \mathfrak{s}(a\alpha)$,

(4) $a\alpha - b\beta$ *is a regular S-pair.*

Proof We prove the contraposition. Assume that there exists a pair $(\beta, b) \in G \times R$ satisfying (3) and (4). This means that $\mathfrak{s}(a\alpha) \succ \mathfrak{s}(b\beta)$ and $\mathrm{LT}(\overline{a\alpha}) = \mathrm{LT}(\overline{b\beta})$. Then, $a\alpha$ is regularly top $\mathfrak{s}$-reducible by $b\beta$. ∎

Lemma 10
Let T be a term in R^m and let G be a signature Gröbner basis up to T. Let α and β in R^m satisfy

(1) $\mathfrak{s}(\alpha) \preceq T$,

(2) α *is completely regular top* $\mathfrak{s}$*-reduced,*

(3) $\mathfrak{s}(\beta) \simeq \mathfrak{s}(\alpha)$,

(4) $\mathrm{LT}(\overline{\beta}) > \mathrm{LT}(\overline{\alpha})$.

Then, β is regularly top $\mathfrak{s}$-reducible.

Proof Assume that β is not regularly top $\mathfrak{s}$-reducible, that is, β is completely regularly top $\mathfrak{s}$-reduced by G. From Lemma 2, we have $\mathrm{LT}(\overline{\beta}) = \mathrm{LT}(\overline{\alpha})$. This contradicts $\mathrm{LT}(\overline{\beta}) > \mathrm{LT}(\overline{\alpha})$. ∎

Lemma 11 means that we do not need to compute terms that do not appear as signatures of regular S-pairs.

Lemma 11
Let T be a term in R^m and let G be a signature Gröbner basis up to T. Let $\alpha \in R^m$ satisfies

(1) $\mathfrak{s}(\alpha) \simeq T$,

(2) $\mathfrak{s}(\alpha)$ *is equivalent to a signature of a regular S-pair that does not appear in Step 3 (ii) (b).*

Let α' be the result of completely regularly top $\mathfrak{s}$-reducing α by G. Then, α' is singularly top $\mathfrak{s}$-reducible by G. In particular, G is a signature Gröbner basis in T.

Proof Let $\beta \in G$ and let a be a monomial in R satisfying $\mathfrak{s}(a\beta) = \mathfrak{s}(\alpha')$ such that $\mathrm{LT}(\overline{a\beta})$ is minimal. We prove that $\mathrm{LT}(\overline{a\beta}) \simeq \mathrm{LT}(\overline{\alpha'})$. By Lemma 8, we have $\mathrm{LT}(\overline{\alpha'}) \leq \mathrm{LT}(\overline{a\beta})$.

Assume that $\mathrm{LT}(\overline{\alpha'}) < \mathrm{LT}(\overline{a\beta})$. By Lemma 10, $a\beta$ is regularly top $\mathfrak{s}$-reducible. Consider $a'\beta$ such that a' is a monomial in R and the monomial $a/a' \in R \setminus K$. Assume that $a'\beta$ is regularly top $\mathfrak{s}$-reducible by G. And let γ be the result of regularly top $\mathfrak{s}$-reducing $a'\beta$. Then, we have $\mathrm{LT}(\overline{a'\beta}) > \mathrm{LT}(\overline{\gamma})$. As $a' < a$, we have $\mathfrak{s}(\gamma) = \mathfrak{s}(a'\beta) \prec \mathfrak{s}(a\beta) \simeq T$. This means that γ is top $\mathfrak{s}$-reducible. However, γ is completely regularly $\mathfrak{s}$-reduced, then γ is singularly top $\mathfrak{s}$-reducible. By Lemma 3, there exists a pair $(\omega, r) \in G \times R$ such that $\mathfrak{s}(\gamma) = \mathfrak{s}(r\omega)$ and $\mathrm{LT}(\overline{\gamma}) = \mathrm{LT}(\overline{r\omega})$. Note that $\mathfrak{s}(a'\beta) = \mathfrak{s}(r\omega)$ and $\mathrm{LT}(\overline{a'\beta}) > \mathrm{LT}(\overline{r\omega})$. By multiplying the both sides of the two equations by a/a', we have $\mathfrak{s}(a\beta) = a/a'\mathfrak{s}(r\omega)$ and $\mathrm{LT}(\overline{a\beta}) > a/a'\,\mathrm{LT}(\overline{r\omega})$ and note that $\frac{a}{a'}$ is a term of R. This means that there exists a pair $(\omega, ar/a') \in G \times R$ such that $\mathfrak{s}((ar/a')\omega) = \mathfrak{s}(a\beta)$ and $\mathrm{LT}(\overline{(ar/a')\omega}) < \mathrm{LT}(\overline{a\beta})$. This contradicts the minimality of $\mathrm{LT}(\overline{a\beta})$.

Therefore, $a'\beta$ with $a/a' \in R \setminus K$ is not regularly top $\mathfrak{s}$-reducible. From Lemmas 7 and 9, there exists an S-pair $a\beta - b\omega'$ such that $\mathfrak{s}(a\beta - b\omega') = \mathfrak{s}(a\beta)$ for $b \in R$ and $\omega' \in G$. This means that a regular S-pair whose signature is $\mathfrak{s}(a\beta) = \alpha$ appears in Step 3 (ii) (b) (#). This is a contradiction. Thus, we have $\mathrm{LT}(\overline{\alpha'}) \simeq \mathrm{LT}(\overline{a\beta})$. Then, α' is singularly top $\mathfrak{s}$-reducible by G.

It follows from Lemma 4 that α' is $\mathfrak{s}$-reduced to $0 \in R$ by G. Thus, G is a signature Gröbner basis in T. ∎

Proposition 12
Let T' in R^m be a term chosen at Step 1 in **Algorithm 2**, *and let T be the term chosen just before T'. Assume that G in* **Algorithm 2** *is a signature Gröbner basis in T after Step 3 of the loop starting with $\alpha = T$. Then, G is a signature Gröbner basis in T' after Step 3 of the loop starting with $\alpha = T'$.*

Proof First, we prove that G is a signature Gröbner basis up to T' when T' is chosen in Step 1. Suppose G is not a signature Gröbner basis up to T'. Consider the set of terms $\alpha \in R^m$ with $T \prec \alpha \prec T'$ satisfying that G is not a signature Gröbner basis in α. Let α_0 be the minimal element of the set. Note that any set of terms in R^m has a minimal element. Then, G is a signature Gröbner basis up to α_0. Because α_0 is not selected before T' is selected, an S-pair whose signature is equivalent to α_0 does not appear in the algorithm. By Lemma 11, G is a signature Gröbner basis in α_0. This contradicts that G is not a signature Gröbner basis in α_0. Therefore, G is a signature Gröbner basis up to T'. The operation on G for T' in **Algorithm 2** is exactly same as that in **Algorithm 1**. By Proposition 5, G is a signature Gröbner basis in T' after Step 3 of the loop starting with $\alpha = T'$. ∎

Our proof of termination is similar to the papers Eder-Perry [5], Roune-Stillman [3] and Eder-Roune [6].

Proposition 13 (Termination)
simpleSB *terminates in finite steps.*

Proof We write $R = K[x_1, \ldots, x_k]$. Set

$$R' = K[x_1, \ldots, x_k, y_{11}, \ldots, y_{mk}, z_1, \ldots, z_m].$$

For $\beta \in R^m$, we write $(\mathfrak{s}(\beta), \mathrm{LT}(\overline{\beta})) = (cx_1^{v_1}x_2^{v_2}\cdots x_k^{v_k}\mathbf{e}_i, r)$, where $c \in K$, $v = (v_1, \ldots, v_k) \in \mathbb{Z}_{\geq 0}^k$ and r is a term of R. Let $f : R^m \to R'$ be the map defined by $\beta \mapsto r y_{i1}^{v_1} \cdots y_{ik}^{v_k} z_i$. Let $G(\alpha)$ be the G (in Algorithm 2) obtained when Step 3 is finished for α, where α was chosen in Step 1. Consider the following monomial ideal $I(\alpha) = \langle f(\beta) \mid \beta \in G(\alpha) \rangle$.

Let $\alpha_1, \alpha_2, \ldots$ be the elements chosen in this order in Step 1 of Algorithm 2. Then we have the sequence $G(\alpha_1) \subset G(\alpha_2) \subset \cdots$ and also $I(\alpha_1) \subset I(\alpha_2) \subset \cdots$. Any ascending sequence of ideals in R' is stable since R' is a Noetherian ring. There exists i_0 such that for $i > i_0$ we have $I(\alpha_i) = I(\alpha_{i_0})$.

For $i < j$, we claim that $G(\alpha_i) \subsetneq G(\alpha_j)$ if and only if $I(\alpha_i) \subsetneq I(\alpha_j)$. The "if"-part is obvious. We prove the "only if"-part in the following way. Suppose that $G(\alpha_i) \subsetneq G(\alpha_j)$ and $I(\alpha_i) = I(\alpha_j)$. Let $\beta \in G(\alpha_j) \setminus G(\alpha_i)$. By $f(\beta) \in I(\alpha_j) = I(\alpha_i)$, there exists $\beta' \in G(\alpha_i)$ such that $f(\beta') | f(\beta)$, since $I(\alpha_i)$ is the ideal generated by the monomials $f(\beta'')$ for $\beta'' \in G(\alpha_i)$. If $f(\beta') \mid f(\beta)$, we have $\mathrm{LT}(\overline{\beta'}) \mid \mathrm{LT}(\overline{\beta})$ and $\mathfrak{s}(\beta') \mid \mathfrak{s}(\beta)$, by the definition of f. Hence, there exist elements β and β' of $G(\alpha_j)$ with $\beta \neq \beta'$ such that $\mathrm{LT}(\overline{\beta'}) \mid \mathrm{LT}(\overline{\beta})$ and $\mathfrak{s}(\beta') \mid \mathfrak{s}(\beta)$. This contradicts that **simpleSB** computes a minimal signature Gröbner basis in $\mathfrak{s}(\alpha_j)$.

Thus we have shown that $G(\alpha_i) = G(\alpha_{i_0})$ for $i > i_0$. Hence G in Algorithm 2 does not grow after α_{i_0}, which means that Step 3 (ii) (b) does not occur after α_{i_0} and therefore P does not grow after α_{i_0}. However, in Step 1, the number of elements in P decreases by one in each step. Thus, Algorithm 2 terminates in finite steps. ∎

Proposition 14 (Correctness)
simpleSB *outputs a signature Gröbner basis when* **simpleSB** *terminates.*

Proof Let T be the term in R^m chosen in Step 1, and finally computed before **simpleSB** terminates. By Proposition 12, G is a signature Gröbner basis in T. Suppose G is not a signature Gröbner basis. Consider the set of terms $\alpha \in R^m$ with $T \prec \alpha$ satisfying that G is not a signature Gröbner basis in α. Let α_0 be the minimal element of the set. Then, G is a signature Gröbner basis up to α_0. However, an S-pair whose signature is equivalent to α_0 does not appear in the algorithm because the algorithm terminates at T. By Lemma 11, G is a signature Gröbner basis in α_0. This contradicts that G is not a signature Gröbner basis in α_0. Therefore, G is a signature Gröbner basis. ∎

5 Simple syzygy signature-based algorithm

In this section, one of the methods to detect zero reductions like F5 and GVW is described. By Lemma 2, because of $\overline{f_i \mathbf{e}_j - f_j \mathbf{e}_i} = 0$, elements in R^m whose signatures are $\mathfrak{s}(f_i \mathbf{e}_j - f_j \mathbf{e}_i)$ are completely regularly $\mathfrak{s}$-reduced to $0 \in R$. Moreover, because of $\overline{r(f_i \mathbf{e}_j - f_j \mathbf{e}_i)} = 0$ for all $r \in R \setminus \{0\}$, elements in R^m whose signatures are $\mathfrak{s}(r(f_i \mathbf{e}_j - f_j \mathbf{e}_i))$ are completely regularly $\mathfrak{s}$-reduced to $0 \in R$. In summary, we have :

Proposition 15
Let T be a term in R^m and let G be a signature Gröbner basis up to T. Let $\alpha, \beta, \gamma \in R^m$ satisfy $\mathfrak{s}(\alpha) \preceq T$ and $\mathfrak{s}(\overline{\beta}\gamma - \overline{\gamma}\beta) \mid \mathfrak{s}(\alpha)$. Then, α is completely regularly $\mathfrak{s}$-reduced to $0 \in R$ by G.

Proof Let r be a monomial in R such that $\mathfrak{s}(\alpha) = \mathfrak{s}(r(\overline{\beta}\gamma - \overline{\gamma}\beta))$. Let α' be the element obtained by completely regularly $\mathfrak{s}$-reducing α. Note that $r(\overline{\beta}\gamma - \overline{\gamma}\beta)$ is the completely regularly $\mathfrak{s}$-reduced element by G because $\overline{r(\overline{\beta}\gamma - \overline{\gamma}\beta)} = 0$. By Lemma 2, we have $\mathrm{LT}(\overline{\alpha'}) = \mathrm{LT}(\overline{r(\overline{\beta}\gamma - \overline{\gamma}\beta)}) = 0$. Then, α is completely regularly $\mathfrak{s}$-reduced to $0 \in R$ by G. ∎

The next proposition gives a method to detect zero reductions, namely it gives a sufficient condition for $\beta \in R$ to be completely regularly s-reduced to $0 \in R$ by G, by means of the term α which has been completely regularly $\mathfrak{s}$-reduced to $0 \in R$.

Proposition 16
Let T be a term in R^m and let G be a signature Gröbner basis up to T. Let α and β in R^m satisfy

(1) α *is completely regularly* $\mathfrak{s}$*-reduced to* $0 \in R$ *by* G *and*

(2) $\mathfrak{s}(\alpha) \mid \mathfrak{s}(\beta)$.

Then, β *is completely regularly* $\mathfrak{s}$*-reduced to* $0 \in R$ *by* G.

Proof From the assumption, there exists $\gamma \in R^m$ such that $\mathfrak{s}(\alpha - \gamma) = \mathfrak{s}(\alpha)$ and $\overline{\alpha - \gamma} = 0$. Let $r \in R$ satisfy $\mathfrak{s}(\beta) = r\mathfrak{s}(\alpha)$. Then, $\mathfrak{s}(r(\alpha - \gamma)) = \mathfrak{s}(r\alpha) = \mathfrak{s}(\beta)$ and $\overline{r(\alpha - \gamma)} = 0$. By Lemma 2, β is completely regularly $\mathfrak{s}$-reduced to $0 \in R$ by G. ∎

Algorithm 3 is simple syzygy signature-based algorithm (**syzSB**). **syzSB** is modified **simpleSB** as to Propositions 15 and 16.

Algorithm 3 Simple syzygy signature-based algorithm (**syzSB**)

Input : a finite subset $F = \{f_1, \ldots, f_m\}$ of R.
Output: a minimal signature Gröbner basis G of F.

Step 0 $G \leftarrow \emptyset, P \leftarrow \{\mathbf{e}_1, \ldots, \mathbf{e}_m\}, H \leftarrow \emptyset$
Step 1 If $P = \emptyset$, return G
$\alpha \leftarrow$ the minimal term in P
$P \leftarrow P \backslash \{\alpha\}$
Step 2 If there exists $\gamma \in H$ with $\gamma \mid \alpha$, go to Step 1
Step 3 $\alpha' \leftarrow$ result of completely regularly top $\mathfrak{s}$-reducing α by G
Step 4 (i) If $\overline{\alpha'} = 0$
$H \leftarrow H \cup \{\alpha\}$
Go to Step 1
(ii) If $\overline{\alpha'} \neq 0$
(a) If α' is singularly top $\mathfrak{s}$-reducible by G
Go to Step 1
(b) If α' is not singularly top $\mathfrak{s}$-reducible by G
$P \leftarrow P \cup \{\mathfrak{s}(\mathrm{spair}(\alpha', \beta)) \mid \beta \in G, \mathrm{spair}(\alpha', \beta) \text{ is regular}\}$ (#)
$H \leftarrow H \cup \{\mathfrak{s}(\overline{\beta}\alpha' - \overline{\alpha'}\beta) \mid \beta \in G\}$
$G \leftarrow G \cup \{\alpha'\}$
Go to Step 1

Proposition 17 (Correctness)
syzSB *outputs a signature Gröbner basis.*

Proof Let A be the set of the terms which **simpleSB** computes, and let B the set of the terms which are completely regularly $\mathfrak{s}$-reduced to $0 \in R$ by G. By Propositions 15 and 16, **syzSB** computes the set $A \setminus B$. Then, the output G of **syzSB** is the same as that of **simpleSB**. ∎

Proposition 18 (Termination)
syzSB *terminates in finite loops.*

Proof By Propositions 15 and 16, the set P at each step 1 in **syzSB** is exactly same as that at the corresponding Step 1 in **simpleSB**. Further, **simpleSB** computes finite number of the terms. ∎

6 Alternative rewrite basis algorithm

In this section, alternative rewrite basis algorithm (**altRB**) is introduced. In the paper [6], rewrite basis algorithm (**RB**) is introduced as a generalized signature-based algorithm. **altRB** is represented easily to understand operations of the algorithm and easily to implement it. It is the most useful signature-based algorithm for implementation in this paper. From the discussion so far, singularly top $\mathfrak{s}$-reducible elements which are completely regularly top $\mathfrak{s}$-reduced need not be included in G. We can expect to improve the algorithm by discarding such elements without reduction. In other words, it is enough to regularly $\mathfrak{s}$-reduce the elements which will be an elements of a minimal signature Gröbner basis. Moreover, we can expect to improve the efficiency by replacing the element α for the element whose signature is the same and which is not needed to reduce more times . Among the algorithms proposed so far, the algorithm in paper [1], GVW [13], etc. have used the method. The paper [7] introduced such algorithms as **RB** with RAT selected for rewrite order. When we choose RAT for a rewrite order, rewrite basis algorithm becomes the most efficient. **altRB** is simply introduced and as efficient as **RB** with RAT. **Algorithm 4** is the pseudocode of **altRB**.

Algorithm 4 Alternative rewrite basis algorithm (**altRB**)

Input : a finite subset $F = \{f_1, \ldots, f_m\}$ of R.
Output: a minimal signature Gröbner basis G of F.

Step 0 $G \leftarrow \emptyset, P \leftarrow \{\mathbf{e}_1, \ldots, \mathbf{e}_m\}, H \leftarrow \emptyset$
Step 1 If $P = \emptyset$, return G
$\alpha \leftarrow$ the minimal term in P
$P \leftarrow P \backslash \{\alpha\}$
Step 2 If there exists $\gamma \in H$ with $\gamma \mid \alpha$, go to Step 1
Step 3 $\alpha' \leftarrow \omega \in \{\alpha\} \cup \{r\beta \mid r \in R, \beta \in G, \mathfrak{s}(r\beta) = \alpha\}$ such that $\mathrm{LT}(\overline{\omega})$ is minimal
Step 4 $\alpha'' \leftarrow$ result of completely regularly top $\mathfrak{s}$-reducing α' by G
Step 5 (i) If $\overline{\alpha''} = 0$
Append α to H
(ii) If $\overline{\alpha''} \neq 0$ and (α' is regularly top $\mathfrak{s}$-reduced at least one time or $\mathfrak{s}(\alpha'')$ is a standard basis)
$P \leftarrow P \cup \{\mathfrak{s}(\mathrm{spair}(\alpha'', \beta)) \mid \beta \in G, \mathrm{spair}(\alpha'', \beta) \text{ is regular}\}$ (#)
$H \leftarrow H \cup \{\mathfrak{s}(\overline{\beta}\alpha'' - \overline{\alpha''}\beta) \mid \beta \in G\}$ $(*)$
$G \leftarrow G \cup \{\alpha''\}$
Go to Step 1

Remark : In Step 4, we execute only regularly "top" $\mathfrak{s}$-reduction according to the description of the algorithm. However, we can execute regularly "tail" $\mathfrak{s}$-reduction, and correctness and termination of the algorithm are not affected. For (#), it is sufficient to leave only one term α in P as for the terms $\alpha \simeq \beta$. Although it is not efficient, if more than two terms are left, correctness and termination of the algorithm are not affected.

Lemma 19
Let α' and α'' be obtained at Step 3 and at Step 4 in **Algorithm 4** *respectively. Let G be a signature Gröbner basis up to $\mathfrak{s}(\alpha'')$. The condition at Step 5 (ii) in* **Algorithm 4** *is equivalent to the condition that α'' is not singularly top $\mathfrak{s}$-reducible by G.*

Proof If $\mathfrak{s}(\alpha'')$ is a standard basis of R^m, say $\mathbf{e}_i$, there is no element in G whose signature belongs to $R\mathbf{e}_i$. Thus, α'' is not singularly top $\mathfrak{s}$-reducible by G. If α' is regularly top $\mathfrak{s}$-reduced at least one time at Step 4, we have $\mathrm{LT}(\overline{\alpha''}) < \mathrm{LT}(\overline{\alpha'})$. For all $b \in R$ and $\beta \in G$ such that $\mathfrak{s}(\alpha'') = \mathfrak{s}(b\beta)$, we have $\mathrm{LT}(\overline{\alpha''}) < \mathrm{LT}(\overline{\alpha'}) \leq \mathrm{LT}(\overline{b\beta})$ by the minimality of $\mathrm{LT}(\overline{\alpha'})$ at Step 3. Then, α'' is not singularly top $\mathfrak{s}$-reducible by G.

Conversely, if α'' is not singularly top $\mathfrak{s}$-reducible, we consider the following two cases : **(a)** $\mathfrak{s}(\alpha'')$ is not a standard basis of R^m and **(b)** otherwise. In case **(a)**, we claim that there exists a pair $(\beta, a) \in G \times R$ with $\mathfrak{s}(\alpha'') = \mathfrak{s}(a\beta)$. Let the signature of α'' be $r\mathbf{e}_i$ ($r \in R \setminus K^\times$). The standard basis of R^m $\mathbf{e}_i$ is chosen at Step 1 before $r\mathbf{e}_i$ is chosen because $\mathbf{e}_i$ is smaller than $r\mathbf{e}_i$. Assume that there does not exist an element of G whose signature is $\mathbf{e}_i$. The element whose signature is $\mathbf{e}_i$ is regularly $\mathfrak{s}$-reduced to $0 \in R$, then we proceed Step 5 (i). In this case, elements whose signatures are $r\mathbf{e}_i$ do not appear in P. This means that we do not compute such an element $r\mathbf{e}_i$. It contradicts that the signature of α'' is $r\mathbf{e}_i$ ($r \in R \setminus K^\times$). Then, there is an element of G whose signature is $\mathbf{e}_i$. Thus, $(r, \mathbf{e}_i)$ is a pair that we claimed. Consider the set of pairs $(\beta, a) \in G \times R$ with $\mathfrak{s}(\alpha'') = \mathfrak{s}(a\beta)$. Let (β', a') be a pair such that $\mathrm{LT}(\overline{a'\beta'})$ is minimal in the set. Note that $\mathrm{LT}(\overline{a\beta}) = \mathrm{LT}(\overline{\alpha'})$ because of the process at Step 3. By Lemma 8, we have $\mathrm{LT}(\overline{\alpha''}) \leq \mathrm{LT}(\overline{a\beta})$. If $\mathrm{LT}(\overline{\alpha''}) = \mathrm{LT}(\overline{a\beta})$, α'' is singularly top $\mathfrak{s}$-reducible. This contradicts that α'' is not singularly top $\mathfrak{s}$-reducible. Then, we have $\mathrm{LT}(\overline{\alpha''}) < \mathrm{LT}(\overline{a\beta}) = \mathrm{LT}(\overline{\alpha'})$. This means that α' is regularly top $\mathfrak{s}$-reduced at least one time at Step 4. In case **(b)**, there is nothing to prove. ∎

Theorem 20 (Correctness)
altRB *outputs a signature Gröbner basis.*

Proof We prove by confirming the difference between the algorithm and the **syzSB**. At Step 3, by Lemma 2, as long as the signature is the same, we can choose any elements in R^m. Thus, we can choose the element with the smaller leading term.

At Step 5, **altRB** does not have branch whether α'' is singularly top $\mathfrak{s}$-reducible or not. Instead of the above, **altRB** check whether α' is regularly top $\mathfrak{s}$-reduced at least one time at Step 4 and check whether $\mathfrak{s}(\alpha'')$ is a standard basis of R^m. By Lemma 19, they are equivalent. ∎

Theorem 21 (Termination)
altRB *terminates in finite steps.*

Proof The set P at every step 1 in **altRB** is exactly same as that at the corresponding Step 1 in **syzSB**. Further, **syzSB** computes finite number of the terms. ∎

7 Module orders and zero reductions

In the paper [7], **RB** does not contain the line $(*)$ of **Algorithm 4**. This is because **RB** is introduced as a generalized signature-based algorithm. If we implement as so, we have to be careful for the number of zero reductions during the calculation. In case we choose POT as a module order and compute incrementally, like **Algorithm 4**, the number of zero reductions becomes small. Especially, if the polynomial systems are regular sequences, the number of zero reductions is zero. In case we choose a module order other than POT or a module order not to be suitable for incremental computation, the number of zero reductions increases during calculation.

It can be proved that the update of H is sufficient to be done first as in **Algorithm 5** in case POT is chosen as the module order and it is calculated incrementally,

Algorithm 5 Alternative rewrite basis algorithm (incremental)

Input : a Gröbner basis $F = \{f_1, \ldots, f_{m-1}\} \subset R$, a polynomial $f_m \in R$.
Output: a minimal signature Gröbner basis G of $F \cup \{f_m\}$.

Step 0 $G \leftarrow \{f_1, \ldots, f_{m-1}\}, P \leftarrow \{\mathbf{e}_m\}, H \leftarrow \{\mathfrak{s}(\overline{\mathbf{e}_i}\mathbf{e}_m - \overline{\mathbf{e}_m}\mathbf{e}_i) \mid 1 \leq i \leq m-1\}$
Step 1 If $P = \emptyset$, return G
$\alpha \leftarrow$ the minimal term in P
$P \leftarrow P \backslash \{\alpha\}$
Step 2 If there exists $\gamma \in H$ with $\gamma \mid \alpha$, go to Step 1
Step 3 $\alpha' \leftarrow \omega \in \{\alpha\} \cup \{r\beta \mid r \in R, \beta \in G, \mathfrak{s}(r\beta) = \alpha\}$ such that $\mathrm{LT}(\overline{\omega})$ is minimal
Step 4 $\alpha'' \leftarrow$result of completely regularly top $\mathfrak{s}$-reducing α' by G
Step 5 (i) If $\overline{\alpha''} = 0$
Append α to H
(ii) If $\overline{\alpha''} \neq 0$ and (α' is regularly top $\mathfrak{s}$-reduced at least one time or $\mathfrak{s}(\alpha'')$ is a standard basis)
$P \leftarrow P \cup \{\mathfrak{s}(\mathrm{spair}(\alpha'', \beta)) \mid \beta \in G, \mathrm{spair}(\alpha'', \beta) \text{ is regular}\}$ (#)
$G \leftarrow G \cup \{\alpha''\}$
Go to Step 1

Lemma 22
Let α'' be a new element at Step 5 (ii) in **Algorithm 5** *with POT such that $\mathbf{e}_1 \prec \mathbf{e}_2 \prec \cdots \prec \mathbf{e}_m$. For all $\beta \in G$, there exists $\gamma \in H$ such that $\gamma \mid \mathfrak{s}(\overline{\alpha''}\beta - \overline{\beta}\alpha'')$.*

Proof First, we prove $H = \{r\mathbf{e}_m \mid r \in \mathrm{HT}(F)\}$. We have $\mathfrak{s}(\overline{\mathbf{e}_i}\mathbf{e}_m - \overline{\mathbf{e}_m}\mathbf{e}_i) = \mathfrak{s}(\overline{\mathbf{e}_i}\mathbf{e}_m)$ because the module order is POT. Then, we have $\mathfrak{s}(\overline{\mathbf{e}_i}\mathbf{e}_m) = \mathfrak{s}(f_i\mathbf{e}_m) = \mathfrak{s}(\mathrm{HT}(f_i)\mathbf{e}_m) = \mathrm{HT}(f_i)\mathbf{e}_m$.

Let α'' and $\beta \in G$ be written as $\alpha'' = \sum_{i=1}^{m} r_i\mathbf{e}_i$ and $\beta = \sum_{j=1}^{m} r'_j\mathbf{e}_j$, for $r_i, r'_i \in R$. Then, we have $\overline{\alpha''} = \sum_{i=1}^{m} r_i f_i \equiv h_m f_m \pmod{F}$.

$$\begin{aligned}\overline{\alpha''}\beta - \overline{\beta}\alpha'' &= \left(\sum_{i=1}^{m} r_i f_i\right) \cdot \left(\sum_{j=1}^{m} r'_j\mathbf{e}_j\right) - \left(\sum_{j=1}^{m} r'_j f_j\right) \cdot \left(\sum_{i=1}^{m} r_i\mathbf{e}_i\right) \\ &= \left\{\left(\sum_{i=1}^{m} r_i f_i\right) \cdot r'_m - \left(\sum_{j=1}^{m} r'_j f_j\right) \cdot r_m\right\}\mathbf{e}_m + \cdots\end{aligned}$$

We focus on polynomial part of $\mathbf{e}_m$.

$$\begin{aligned}\left(\sum_{i=1}^{m} r_i f_i\right) \cdot r'_m - \left(\sum_{j=1}^{m} r'_j f_j\right) \cdot r_m &\equiv r_m f_m r'_m - r'_m f_m r_m \pmod{F} \\ &\equiv 0 \pmod{F}\end{aligned}$$

Therefore, there exists an element in H which divides $\mathfrak{s}(\overline{\alpha''}\beta - \overline{\beta}\alpha'')$. ∎

8 Conclusion

We have presented some signature-based (semi-)algorithms for computing Gröbner bases: **fundSB**, **simpleSB**, **syzSB** and **altRB**. Among them, **altRB** is a practical signature-based algorithm and can

be implemented easily in any computer algebra system, as **altRB** is described concretely. The other (semi-)algorithms are used auxiliarily to prove the correctness and the termination of **altRB**. The characteristics of the (semi-)algorithms are as follows:

1. **fundSB** is a prototype of signature-based algorithms, and helps us grasp the idea and how signature-based algorithms work. However, it does not terminate.
2. **simpleSB** is obtained by modifying **fundSB** with the concept of S-pairs so that it terminates. It outputs a signature Gröbner basis with a finite number of operations.
3. **syzSB** is obtained by including a step detecting zero reductions into **simpleSB**. The step is assured by Propositions 15 and 16.
4. **altRB** is obtained by inserting in **syzSB** a step replacing the term by an element which has a smaller leading term. This enables us to reduce the number of regular $\mathfrak{s}$-reductions significantly.

By discussing the correctness and the termination of these (semi-)algorithms step by step, we have finally obtained the correctness and the termination of **altRB**. The proofs are self-contained and very clear. **altRB** is efficient for an arbitrary module order. In the last section, we have discussed how signature-based algorithms work when POT is chosen as a module order and when it proceeds incrementally.

As a future work, it would be meaningful to study the relation between input systems and module orders we choose, toward finding an efficient module order for a given input system.

Acknowledgement

This paper is a part of the dissertation written by the author under the supervision by Prof. Shushi Harashita. The author thanks him for his constant supports. The author thanks Prof. Kazuhiro Yokoyama and Prof. Masayuki Noro for discussions on the topic of this manuscript. The author is grateful to the anonymous referees for their helpful and kind comments. A part of this work has been supported by Joint research promotion program of Graduate School of Environment and Information Sciences, Yokohama National University.

References

[1] Arri, A., Perry, J.: The F5 criterion revised.: *Journal of Symbolic Computation*, **46**, 1017–1029, 2011.

[2] Buchberger, B.: Bruno Buchberger's Ph.D. thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal.: *Journal of Symbolic Computation*, **41**, 475–511, 2006. https://doi.org/10.1016/j.jsc.2005.09.007

[3] Roune, B.H., Stillman, M.: Practical Gröbner basis computation.: Proceedings of the 2012 International Symposium on Symbolic and Algebraic Computation , 203–210, ACM, New York, 2012. https://arxiv.org/abs/1206.6940 (extended version)

[4] Eder, C., Perry, J.: F5C: a variant of Faugère's F5 algorithm with reduced Gröbner bases.: *Journal of Symbolic Computation*, **45**, no. 12, 1442–1458, 2010.

[5] Eder, C., Perry, J.: Modifying Faugère's F5 algorithm to ensure termination.: *ACM SIGSAM Commun. Comput. Algebra*, **45**, 70–89, 2011.

[6] Eder, C., Roune, B.H.: Signature rewriting in Gröbner basis computation.: Proceedings of the 2013 International Symposium on Symbolic and Algebraic Computation, 331–338, 2013.

[7] Eder, C., Faugère, J.-C.: A survey on signature-based algorithms for computing Gröbner bases.: *Journal of Symbolic Computation*, **80**, part 3, 719–784, 2017.

[8] Ars, G., Hashemi, A.: Extended F5 criteria.: *Journal of Symbolic Computation*, **45** (12) , 1330–1340, 2010.

[9] Faugère, J.-C.: A new efficient algorithm for computing Gröbner bases without reduction to zero (F5).: Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation, 75–83, ACM, New York, 2002.

[10] Faugère, J.-C., Joux, A.: Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases.: CRYPTO 2003, Advances in Cryptology, vol. 2729, 44–60, 2003.

[11] Pan, S., Hu, Y., Wang, B.: The termination of algorithms for computing Gröbner bases.: 2010. http://arxiv.org/abs/1202.3524

[12] Galkin, V.: Termination of original F5.: 2012. http://arxiv.org/abs/1203.2402

[13] Gao, S., Volny, F. IV, Wang, M.: A new framework for computing Gröbner bases.: *Mathematics of Computation*, **85**, 449–465, 2016. https://doi.org/10.1090/mcom/2969

[14] Vaccon, T., Yokoyama, K.: A tropical F5 algorithm.: Proceedings of the 2017 International Symposium on Symbolic and Algebraic Computation, 429–436, ACM, 2017.

[15] Vaccon, T., Verron, T., Yokoyama, K.: On Affine Tropical F5 Algorithms.: Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation, 383–390, ACM, 2018.

Communications of JSSAC Vol. 4 2020
Publisher Japan Society for Symbolic and Algebraic Computation
Office zip 102–0074
Resona Kudan Building 5F KS Floor, 1-5-6 Kudanminami Chiyoda-ku Tokyo, Japan