J. Symbolic Computation (1999) **28**, 243–263
Article No. jsco.1998.0275
Available online at http://www.idealibrary.com on IDEAL®

A Modular Method to Compute the Rational Univariate Representation of Zero-dimensional Ideals

MASAYUKI NORO[†] AND KAZUHIRO YOKOYAMA[‡]

High Performance Computing Research Center, Fujitsu Laboratories Ltd.
1-1 Kamikodanaka 4-Chome, Nakahara-ku, Kawasaki 211-8588, Japan

To give an efficiently computable representation of the zeros of a zero-dimensional ideal I, Rouillier (1996) introduced the rational univariate representation (RUR) as an extension of the generalized shape lemma (GSL) proposed by Alonso *et al.* (1996). In this paper, we propose a new method to compute the RUR of the radical of I, and report on its practical implementation. In the new method, the RUR of the radical of I is computed efficiently by applying modular techniques to solving the systems of linear equations. The performance of the method is examined by practical experiments. We also discuss its theoretical efficiency.

1. Introduction

To express all zeros of a zero-dimensional ideal I in a polynomial ring $\mathbb{Q}[X]$ over the rational number field $\mathbb{Q}$, several researchers studied the Gröbner basis of I with respect to a lexical (lexicographical) order. For example, in a *special case*, the Gröbner basis with respect to some lexical order has the following form suited to express the zeros:

$$\{g(x_1), x_2 - h_2(x_1), \ldots, x_n - h_n(x_1)\}, \tag{1.1}$$

where $X = \{x_1, \ldots, x_n\}$, $g, h_2, \ldots, h_n$ are univariate polynomials over $\mathbb{Q}$. We call the base (1.1) the *shape base* (Gianni and Mora, 1989; Becker *et al.*, 1994). To improve the efficiency of the Gröbner basis computation, Buchberger (1965, 1970) and Kobayashi *et al.* (1988) proposed *change of ordering* methods and Faugère *et al.* (1993) improved the methods. These methods compute the Gröbner basis of I with respect to the desired order by solving systems of linear equations derived from the ideal membership of elements. This procedure corresponds to solving a system of linear equations by Gaussian elimination, which may cause intermediate swells even if one uses fraction-free Gaussian elimination and even if each entry of the solution is small. Moreover, the solution often has very huge entries which make the computation of the desired Gröbner basis hard.

On the other hand, to give a compact representation of the zeros of I, Alonso *et al.*

[†] E-mail: noro@para.flab.fujitsu.co.jp
[‡] E-mail: yokoyama@para.flab.fujitsu.co.jp

0747–7171/99/070243 + 21 $30.00/0

(1996) proposed to express the zeros by the *generalized shape lemma (GSL)*. This method represents the radical $\sqrt{I}$ of a given ideal I as

$$\sqrt{I} = Id(g(u), g'(u)x_1 - h_1(u), \dots, g'(u)x_n - h_n(u)), \tag{1.2}$$

where $g, h_1, \dots, h_n$ are univariate polynomials over $\mathbb{Q}$, and g' is the derivative of g. Here, we call the generating set in (1.2) the *GSL form* of I with respect to u and call u a *separating element.* It is empirically known that coefficients of elements in the GSL form are often very small compared with those in the Gröbner basis with respect to the lexical order. Recently, González-Vega and Trujillo (1995) and Rouillier (1996) applied symmetric function methods to compute the GSL form. To handle non-radical ideals uniformly, Rouillier (1996) extended the notion of GSL and proposed a new method to express each zero of I by a rational function in a separating element. We call such a form the *rational univariate representation (RUR).* If I is radical, the RUR of I coincides with the GSL form of I. Here, we consider the notion of RUR as a general mathematical notion containing GSL form, and so we call the GSL form of I *the RUR of the radical* of I. And if I is radical, we simply call the GSL form the *RUR* of I.

In this paper we apply the modular techniques used in Noro and Yokoyama (1995), to give a new method to compute the *RUR of the radical* of a given ideal I. In many cases arising from practical problems, where the ideal has a shape base, the new method computes the RUR efficiently. As for general cases, we have to compute various ideal bases or ideal quotients. The modular techniques are also useful for such computations and the RUR of the radical is computed efficiently by combining them. Although theoretically the new method computes the RUR along with the radical, actually we compute the ideal quotient instead of the radical, which enables us to apply the modular techniques. Especially, if the ideal is radical, ideal quotient computations are not necessary and the computation of the RUR is simplified.

Here, the modular techniques used are threefold: (1) the guess of a separating element, which is also used in Rouillier's method; (2) the guess of the form of the result, where we provide several criteria for checking the correctness of the guess; and (3) the lifting of the solution of a system of linear equations from its modular solution, which is newly introduced in this paper. Concerning (1), we can check if the given ideal I has a shape base at the same time. After determining the form of the result, we express the result as the unique solution of the system of linear equations. In a "well situation", the modular solution coincides with the modular image of the correct solution and it can be obtained by an ordinary lifting procedure. In order to make sure of such a well situation, we need the notion of "compatibility" of a prime p, which gives mathematical foundations concerned with the correspondence between Gröbner bases in $\mathbb{Q}[X]$ and those in $GF(p)[X]$.

We test the new method for several examples on a real computer, by which certain evidence of the efficiency is obtained. Even though the computation of a Gröbner basis is rather hard and it dominates the additional computations for the RUR in general, improving the RUR computation should contribute the total efficiency.

This paper is organized as follows. In Section 2 we provide foundations of modular techniques. We show the correspondence between Gröbner bases in $\mathbb{Q}[X]$ and those in $GF(p)[X]$ under the compatibility, and the reduction of the problem to the solving of systems of linear equations. In Section 3 we give our new method to compute the RUR of the radical of a given zero-dimensional ideal. In Section 4 we discuss how to find separating elements and in Section 5 we show the timings of experiments. Finally, in Section 6, we give the estimate of the complexity and characterize the new method.

2. Foundation of Modular Method

We begin by summarizing the modular method for change of ordering of Gröbner bases in Noro and Yokoyama (1995). The following notations will be used:

Notation 2.1. $\mathbb{Q}$: the field of rational numbers.
$\mathbb{Z}$: the ring of rational integers.
p : a prime number.
$GF(p)$: the finite field of order p.
K: a perfect field either $\mathbb{Q}$ or $GF(p)$.
$\mathbb{Z}_{<p>} = \{a/b | a \in \mathbb{Z}; b \in \mathbb{Z} \setminus p\mathbb{Z}\} \subset \mathbb{Q}$: the localization of $\mathbb{Z}$ at $< p >= p\mathbb{Z}$.
$X = \{x_1, \dots, x_n\}$: indeterminates.
ϕ_p : the canonical projection from $\mathbb{Z}_{<p>}[X]$ to $GF(p)[X]$. Thus $\phi_p(a/b) = \phi_p(a)/\phi_p(b)$ for $a \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus p\mathbb{Z}$.
$<$, $<_0$: admissible orders.
$ht_<(f)$: the head term (the leading power product) of a polynomial f with respect to $<$.
$hc_<(f)$: the head coefficient of a polynomial f with respect to $<$.
$GB_<(I)$: the reduced Gröbner basis of an ideal I.
$Id(F)$: the ideal generated by a polynomial set F in $K[X]$.
$NF_<(f, G)$: a normal form of a polynomial f modulo a polynomial set G with respect to $<$.
$Init_<(I)$: the ideal generated by $\{ht_<(f) | f \in I\}$.
$sq(f)$: the maximal square-free part of a polynomial f.
$support(f)$: the set of all terms appearing in a polynomial f.

2.1. Compatibility and Gröbner bases

Let $F \subset \mathbb{Q}[X]$ be a polynomial set and $I = Id(F)$.

Definition 2.2. (Compatibility of Prime)
(1) A prime p is *compatible* with F if $F \subset \mathbb{Z}_{<p>}[X]$ and $\phi_p(I \cap \mathbb{Z}_{<p>}[X]) = Id(\phi_p(F))$.
(2) A prime p is *strongly compatible* with $(F, <)$ if p is compatible with F and $\phi_p(Init_<(I) \cap \mathbb{Z}_{<p>}[X]) = Init_<(Id(\phi_p(F)))$.
(3) A prime p is *permissible* for $(F, <)$ if for each $f \in F$, $f \in \mathbb{Z}_{<p>}[X]$ and $\phi_p(hc_<(f)) \neq 0$.

Note that the compatibility is independent of the term order, and that the strong compatibility implies the compatibility. From now on, we assume $F \subset \mathbb{Z}_{<p>}[X]$.

Definition 2.3. (Compatible Candidate) A set $G \subset I \cap \mathbb{Z}_{<p>}[X]$ is a *p-compatible Gröbner basis candidate* of I with respect to $<$ if p is permissible for $(G, <)$ and if $\phi_p(G)$ is a Gröbner basis of $\phi_p(I \cap \mathbb{Z}_{<p>}[X])$ with respect to $<$.

We recall the following important results (see Noro and Yokoyama, 1995). Here we assume that in normal form computations, the choice of a reducer depends only on terms in the polynomial to be reduced and on the head term set of the reducers.

LEMMA 2.4. *Let $G \subset \mathbb{Z}_{<p>}[X]$ be a polynomial set and p a prime permissible for $(G,<)$, and $f \in \mathbb{Z}_{<p>}[X]$. Then $NF_<(f,G) \in \mathbb{Z}_{<p>}[X]$ and $NF_<(\phi_p(f),\phi_p(G)) = \phi_p(NF_<(f,G))$.*

PROOF. $NF_<(f,G)$ is computed by the following recurrence:

$$f_0 \leftarrow f, \qquad f_i \leftarrow f_{i-1} - \alpha_i t_i g_{k_i},$$

where $\alpha_i \in \mathbb{Q}$, t_i is a term and $g_{k_i} \in G$ for each i. Then $\alpha_i \in \mathbb{Z}_{<p>}$, because p is permissible for $(G,<)$. Thus $f_i \in \mathbb{Z}_{<p>}[X]$ for all i. Applying ϕ_p for both side of the recurrence, we have $\phi_p(f_i) = \phi_p(f_{i-1}) - \phi_p(\alpha_i)t_i\phi_p(g_{k_i})$. If $\phi_p(\alpha_i) \neq 0$ then $\phi_p(f_{i-1}) \neq 0$ and the step $\phi_p(f_i) \leftarrow \phi_p(f_{i-1}) - \phi_p(\alpha_i)t_i\phi_p(g_{k_i})$ is a head term reduction modulo $\phi_p(G)$. If $\phi_p(\alpha_i) = 0$ then $\phi_p(f_i) = \phi_p(f_{i-1})$. Thus the sequence $\{\phi_p(f_i) | i = 0 \text{ or } \phi_p(\alpha_i) \neq 0\}$ corresponds to the computation of $NF_<(\phi_p(f),\phi_p(G))$. If there exists i such that $\phi_p(f_i) = 0$ then the modular image of the sequence is truncated, but the statement still holds, because $NF_<(\phi_p(f),\phi_p(G)) = \phi_p(NF_<(f,G)) = 0$ for such a case. □

By Lemma 2.4 and the definition of Gröbner basis, we immediately have the following.

COROLLARY 2.5. *Suppose that $G \subset \mathbb{Z}_{<p>}[X]$ is a Gröbner basis of $Id(G)$ with respect to $<$. If p is permissible for $(G,<)$, then $\phi_p(G)$ is a Gröbner basis of $Id(\phi_p(G))$ and p is strongly compatible with $(G,<)$.*

By Corollary 2.5, if F is the Gröbner basis of $Id(F)$ with respect to an order $<_0$, the compatibility of p with F can be determined by checking its permissibility for $(F,<_0)$. A similar result was presented in Gräbe (1993), but the "luckiness"defined there depends on the term order and it is not applicable directly for the change of ordering. On the other hand, under the compatibility, a Gröbner basis candidate, if it exists, is an actual Gröbner basis.

THEOREM 2.6. *If G is a p-compatible Gröbner basis candidate of I with respect to $<$, then G is a Gröbner basis of I with respect to $<$. In particular, if p is compatible with F, p is permissible for $(G,<)$, and $\phi_p(G)$ is a Gröbner basis of $Id(\phi_p(F))$, then G is a Gröbner basis of $Id(F)$ with respect to $<$.*

PROOF. We show that every $f \in I$ is reduced to 0 by G with respect to $<$. We can assume that $f \in I$ is G-reduced. If $f \neq 0$ then, by multiplying a rational number, we may assume that $f \in I\backslash\{0\}$ is a G-reduced integral polynomial, and the content of f, the GCD of the coefficients of f, is equal to 1. Then, $\phi_p(f) \neq 0$ holds, otherwise the content of f would have a factor p. As $\phi_p(f) \in \phi_p(I \cap \mathbb{Z}_{<p>}[X])$, $\phi_p(f)$ must be reduced to 0 by $\phi_p(G)$ with respect to $<$. But f is G-reduced and the set of head terms of $\phi_p(G)$ is the same as that of G. Thus, $\phi_p(f)$ is already $\phi_p(G)$-reduced and $\phi_p(f) = 0$. This is a contradiction. □

In more precise terms, we have the following theorem on subsets of the Gröbner basis.

THEOREM 2.7. *Let $\overline{G} \subset GF(p)[X]$ be the reduced Gröbner basis of $\phi_p(I \cap \mathbb{Z}_{<p>}[X])$ with respect to $<$ and set $\overline{G} = \{\overline{g}_1,\ldots,\overline{g}_s\}$ with $\overline{g}_1 < \ldots < \overline{g}_s$. Let t be a positive integer not greater than s. If there exists $g_i \in I \cap \mathbb{Z}_{<p>}[X]$ for $1 \leq i \leq t$ such that $\phi_p(g_i) = \overline{g}_i$ and g_i*

is $\{g_1, \dots, g_{i-1}\}$-reduced, then $g_1, \dots, g_t$ are the first t-elements of the reduced Gröbner basis of I with respect to $<$.

Next we consider the ideal quotient for an ideal I and a polynomial f. Without loss of generality, we can assume that $\phi_p(f) \neq 0$.

THEOREM 2.8. *Let H be a polynomial set in $\mathbb{Z}_{<p>}[X] \cap (I : f)$. Assume that the fixed prime p is compatible with F and permissible for $(H, <)$, and $\phi_p(H)$ is a Gröbner basis of $(\phi_p(F) : \phi_p(f))$ with respect to $<$. Then H is a p-compatible Gröbner basis candidate of $(I : f)$ with respect to $<$ and so H is a Gröbner basis of $(I : f)$ with respect to $<$.*

PROOF. First we show the following:

CLAIM. $Id(\phi_p(H)) = (\phi_p(F) : \phi_p(f)) = \phi_p((I : f) \cap \mathbb{Z}_{<p>}[X])$.

PROOF OF CLAIM. For $h \in (I : f) \cap \mathbb{Z}_{<p>}[X]$, the fact $hf \in I$ implies that $\phi_p(h)\phi_p(f) \in \phi_p(I \cap \mathbb{Z}_{<p>}[X]) = Id(\phi_p(F))$ and so $\phi_p(h) \in Id(\phi_p(H))$. Thus, $Id(\phi_p(H)) \supset \phi_p((I : f) \cap \mathbb{Z}_{<p>}[X])$. Conversely, for $\bar{h} \in Id(\phi_p(H))$, there is an inverse image $h \in Id(H) \cap \mathbb{Z}_{<p>}[X]$ such that $\bar{h} = \phi_p(h)$. As $H \subset (I : f)$, hf belongs to I and so $\bar{h} = \phi_p(h)$ belongs to $\phi_p((I : f) \cap \mathbb{Z}_{<p>}[X])$. □

By Claim, we conclude that H is a p-compatible Gröbner basis candidate of $(I : f)$. Because $H \subset \mathbb{Z}_{<p>}[X]$, $\phi_p(hc_<(h)) \neq 0$ for $h \in H$ and $Id(\phi_p(H)) = \phi_p((I : f) \cap \mathbb{Z}_{<p>}[X])$. By Theorem 2.6, H is a Gröbner basis of $(I : f)$ with respect to $<$. □

2.2. FINDING ELEMENTS OF SPECIAL FORMS BY MODULAR TECHNIQUES

Suppose that F is a Gröbner basis of an ideal I with respect to a term order $<$ and a prime p is permissible for $(F, <)$. Then p is strongly compatible with F. Here we give a method to find a polynomial in I which has a special form. Now we assume the following:

(1) The head term $t_0 (= ht_<(f))$ is given.
(2) The support $T (= support(f))$ of f is given.

Replacing the coefficient of each term $t = x_1^{e_1} \cdots x_n^{e_n}$ in T with the variable b_t, we have the following equations over $\mathbb{Q}[X]/I$:

$$f_B = \sum_{t \in T} b_t t \equiv 0 \qquad (\text{mod } I).$$

As we already know the Gröbner basis F, this is reduced to the following system of linear equations over $\mathbb{Q}$.

$$\sum_{t \in T} b_t [t] = 0 \qquad \text{with } b_{t_0} = 1, \tag{2.1}$$

where $[g]$ denotes the vector representation of a polynomial g derived from $NF_<(g, F)$. That is, by considering the residue class ring $\mathbb{Q}[X]/I$ as a vector space over $\mathbb{Q}$ whose linear base consists of all terms reduced with respect to F, the residue class containing g is represented as the normal form $NF_<(g, F)$. By Lemma 2.4, ϕ_p and NF commute and we have

$$\sum_{t \in T} b_t \overline{[t]} = 0 \qquad \text{with } b_{t_0} = 1, \tag{2.2}$$

where $\overline{[\bar{g}]}$ denotes the vector representation of a polynomial $\bar{g}$ over $GF(p)$ derived from $NF_<(\bar{g}, \phi_p(F))$. Therefore the computation of a candidate of the modular image of the solution is reduced to an ideal membership problem for $Id(\phi_p(F))$. So we further assume the following.

(3) The system (2.2) has the unique solution $\bar{A}$ and it is already computed.

Then the system (2.1) has at most one solution. We try lifting the p-adic solution to that over $\mathbb{Q}$, starting from $\bar{A}$. This can be done by Hensel lifting. We call this procedure *the method of indeterminate coefficient with modular technique* or simply *the modular method.* (We show the concrete algorithm in the next subsection.)

Now we show two examples. One is "change of ordering" proposed in Noro and Yokoyama (1995) and the other is "ideal quotient", newly introduced in this paper.

Change of ordering: Let F be a Gröbner basis of an ideal I with respect to a term order $<$. We want to compute a Gröbner basis G with respect to another term order $<_1$. In order to compute G we compute p-compatible candidate G'. That is, we construct a system of linear equations for each $\bar{g} \in \bar{G}$. (So, we guess the support of each element of G by that of the corresponding element of $\bar{G}$.)

$$\sum_{t \in support(\bar{g})} b_t[t] = 0 \qquad \text{with } b_{ht_<(\bar{g})} = 1, \tag{2.3}$$

where $[h]$ denotes the vector representation of a polynomial h derived from $NF_<(h, F)$. Here $\bar{G}$ is the reduced Gröbner basis of $Id(\phi_p(F))$ with respect to $<_1$ and the uniqueness of the solution modulo p is guaranteed. Thus, the following holds by Lemma 2.4, Theorem 2.6 and Corollary 2.5.

Proposition 2.9. (1) *If there is a solution, say $A_{\bar{g}}$, over $\mathbb{Z}_{<p>}$ for the equations (2.3) for any element $\bar{g}$ in $\bar{G}$, then the set G' of polynomials corresponding to $A_{\bar{g}}$, $\bar{g} \in \bar{G}$, satisfies the condition of Theorem 2.6 and hence G' is the reduced Gröbner basis of I.*
(2) *If p is permissible for $(GB_{<_1}(I), <_1)$ then the solution always exists. Thus the number of primes p for which the solution does not exist is finite.*

Ideal quotient: As computing ideal quotients can be reduced to solving systems of linear equations (see Lakshman, 1990), the same modular technique is applicable for improving the efficiency. We slightly modify the construction of the system of linear equations as follows.

Let F be a Gröbner basis of an ideal I with respect to a term order $<$. We compute a Gröbner basis H of $(I : f)$ for a polynomial f. Here p is a prime permissible for $(F, <)$, i.e. strongly compatible with $(F, <)$ and f in $\mathbb{Z}_{<p>}[X]$. Then the problem is reduced to solving the following system of linear equations. Let $\bar{H}$ be a Gröbner basis of $(Id(\phi_p(F) : \phi_p(f))$. For each $\bar{h} \in \bar{H}$,

$$\sum_{t \in support(\bar{h})} b_t[ft] = 0 \qquad \text{with } b_{ht_<(\bar{h})} = 1, \tag{2.4}$$

where $[g]$ denotes the vector representation of a polynomial g derived from $NF_<(g, F)$. The solution modulo p corresponds to $\bar{h}$ and the uniqueness of the solution is guaranteed. Thus, the following holds by Lemma 2.4, Theorem 2.8 and Corollary 2.5.

PROPOSITION 2.10. (1) *If there is a solution, say $A_{\bar{h}}$, over $\mathbb{Z}_{<p>}$ for the equations (2.4) for any element $\bar{h}$ in $\bar{H}$, then the set H of polynomials corresponding to $A_{\bar{h}}$, $\bar{h} \in \bar{H}$, satisfies the condition of Theorem 2.8 and hence H is the reduced Gröbner basis of $(I : f)$.* (2) *If p is permissible for $(GB_<(I : f), <)$ then the solution exists and $H = GB_<(I : f)$. Thus the number of primes p for which the solution does not exist is finite.*

2.3. LIFTING BY HENSEL CONSTRUCTION

The system of linear equations can be reduced to its subsystem. After solving the subsystem, if there is a solution, we check if the solution also satisfies the whole system.

PROBLEM 2.11. Solve a system of linear equations $AB = C$ for an unknown vector B, where A is a $d \times d$ matrix and C is a vector over $\mathbb{Z}_{<p>}$, under the assumption $\det(\phi_p(A)) \neq 0$.

We can apply Hensel lifting to solve this system.

ALGORITHM 2.12.

```
solve_linear_equation_by_hensel(A, C, p)
Input : a $d \times d$ matrix $A$, a $d \times 1$ matrix $C$, a prime $p$ such that $\phi_p(\det(A)) \neq 0$
Output : a $d \times 1$ matrix $B$ such that $AB = C$

$R \leftarrow \phi_p(A)^{-1}$; $c \leftarrow C$; $b \leftarrow 0$; $q \leftarrow 1$; count $\leftarrow 0$
do {
    $t \leftarrow \phi_p^{-1}(R\phi_p(c))$; $b \leftarrow b + qt$; $c \leftarrow (c - At)/p$; $q \leftarrow qp$; count $\leftarrow$ count + 1
    ($\phi_p^{-1}$ denotes the canonical inverse image; $(c - At)/p$ is an exact division.)
    if count = Predetermined_Constant then {
      count $\leftarrow 0$; $B \leftarrow$ inttorat$(b, q)$
      if $B \neq$ nil then return $B$
    }
}
```

In Algorithm 2.12, *inttorat*(x, q) executes the rational number reconstruction from x modulo q (Wang *et al.*, 1982) for each entry, and it returns the result if the reconstruction is successful, or **nil** if it failed. Each iteration step is executed within a constant time, and intermediate swells do not occur because the termination depends upon the size of the result.

3. Expressing Zeros of a Zero-dimensional Ideal by its RUR

Here we apply the modular method in Section 2 to compute the RUR of the radical of a given ideal. When we apply the modular method to the computation of change of ordering or that of ideal quotient, the compatibility does not guarantee the existence of the solution. However, for the RUR computation, the existence of the solution of the system of linear equations over $GF(p)$ implies that it also exists over $\mathbb{Q}$ and it can be computed by lifting from the modular solution. In this sense the modular technique is quite suitable for the RUR computation.

First of all we give an algorithm for a special case called the *shape base* case. For general cases, the method for the shape base case cannot be applied directly. However, as what we want to compute is a representation of zeros, we execute ideal decompositions, if possible, and we apply the method for the shape base case to each component. Here we propose a dynamic method which includes a criterion for detecting easy cases such as the shape base case. Note that the method for general cases can compute the RUR efficiently if an input is radical or nearly radical.

We begin by introducing necessary notions in slightly different settings compared with Alonso *et al.* (1996), González-Vega and Trujillo (1995) and Rouillier (1996) to focus the shape base case. From now on, we assume that a given ideal I is zero-dimensional over a perfect field K. (We consider $\mathbb{Q}$ and $GF(p)$ for K.) Let $\bar{K}$ denote the algebraic closure of K.

Definition 3.1. (Linear Map and Minimal Polynomial) (1) For a polynomial f in $K[X]$, a linear map on the residue class ring $K[X]/I$ is defined by

$$K[X]/I \ni u \to fu \in K[X]/I.$$

We call this *the multiplication map* of f on $K[X]/I$ and denote it by $M_{f,I}$.

(2) For a polynomial f in $K[X]$, its minimal polynomial with respect to I is defined as the minimal polynomial of $M_{f,I}$ as a linear map.

It is well known that for any polynomial f in $K[X]$, its minimal polynomial with respect to I coincides with the monic univariate polynomial over K having the smallest degree among all univariate polynomials m such that $m(f)$ belongs to I.

Definition 3.2. (Separating Element) A polynomial f in $K[X]$ is a separating element for I if for every pair (α, β) of distinct zeros of I in $\bar{K}$, $f(\alpha) \neq f(\beta)$.

When I is a radical ideal, f is a separating element for I if and only if the degree of its minimal polynomial coincides with the dimension $\dim_K(K[X]/I)$.

Definition 3.3. (Shape Base and RUR) A generating set G of I is a shape base of I if

$$G = \{g(u), x_1 - g_1(u), \ldots, x_n - g_n(u)\},$$

where $u \in K[X]$ and $g_1, \ldots, g_n$ are univariate polynomials over K of degree less than $\deg(g)$. In this case u is a separating element for I. Moreover, for the shape base G above, if $g(u)$ is square-free, i.e. I is radical, then there is another generating set H called the rational univariate representation (RUR) of I with respect to u such that

$$H = \{g(u), g'(u)x_1 - h_1(u), \ldots, g'(u)x_n - h_n(u)\},$$

where g' is the derivative of g and $h_1, \ldots, h_n$ are univariate polynomials over K of degree less than $\deg(g)$. By the conditions $\deg(g_i) < \deg(g)$, $\deg(h_i) < \deg(g)$, the shape base and the RUR with respect to a fixed u are uniquely determined if exists.

Compared with shape base, RUR has a computational advantage because the coefficients in RUR are often much smaller than those in shape base (see Alonso *et al.*, 1996).

Let G be the shape base of I in the definition. For the ideal I_0 generated by $y - u$ and I in a polynomial ring $K[X \cup \{y\}]$, where y is a new variable, $G_0 = \{g(y), x_1 - g_1(y), \dots, x_n - g_n(y)\}$ is the reduced Gröbner basis with respect to any block order $<'$ with $y << X$. Moreover, we have:

LEMMA 3.4. *If I is radical and $u \in K[X]$ is a separating element, then I has the shape base G with respect to u and the ideal I_0 derived from I also has the shape base which is a Gröbner basis with respect to any block order $<$ with $y << X$. In this case, there are the RUR of I with respect to u and the RUR of I_0 with respect to y.*

From now on, for the sake of simplicity, we deal with the case where the variable x_0 is assigned to a *known* separating element. So, let $X = \{x_0, \dots, x_n\}$, $<_0$ a term order, $<$ the lexical order such that $x_0 < \dots < x_n$, $F \subset \mathbb{Z}_{<p>}[X]$, $I = Id(F)$ and $G = GB_{<_0}(I)$.

REMARK 3.5. From the practical point of view, it is very desirable that a variable is chosen as a separating element. Because if a separating element is chosen from a non-trivial polynomial, it often destroys the sparsity the given ideal originally has, which makes the computation of minimal polynomials hard.

3.1. SHAPE BASE CASE

Under the permissibility, the existence of the modular shape base implies the existences of the shape base and the RUR over $\mathbb{Q}$.

THEOREM 3.6. *Suppose that a prime p is permissible for $(G, <_0)$. If $GB_<(Id(\phi_p(G)))$ is the shape base then $GB_<(I)$ is also the shape basis and $GB_<(I) \subset \mathbb{Z}_{<p>}[X]$. Thus, $GB_<(I)$ is obtained by lifting the modular image $GB_<(Id(\phi_p(G)))$.*

PROOF. Let $\bar{H} = GB_<(Id(\phi_p(G)))$. As $\bar{H}$ is the shape base,

$$\bar{H} = \{\bar{g}(x_0), x_1 - \bar{g}_1(x_0), \dots, x_n - \bar{g}_n(x_0)\}$$

holds. For each element in $\bar{H}$ we construct a system of linear equations and we solve it over $\mathbb{Q}$ by the modular method in Section 2.2. If each solving succeeds, the set of all the solutions forms a p-compatible candidate of I with respect to $<$, and the set H is the Gröbner basis by Theorem 2.7. So, in order to prove the theorem it is sufficient to show that each system of linear equations has always a solution.

LIFTING OF $\bar{g}$: Let $D = \dim_{\mathbb{Q}}(\mathbb{Q}[X]/I)$ and $\bar{g}(x_0)$ is the minimal polynomial of x_0 which is the unique element of $GB_<(Id(\phi_p(G))) \cap GF(p)[x_0]$. (As $GB_<(Id(\phi_p(G)))$ is the shape base, x_0 is a separating element for $Id(\phi_p(G))$.) We construct the following system of linear equations.

$$\sum_{k=0}^{D-1} b_k[x_0^k] + [x_0^D] = 0, \tag{3.1}$$

where $[h]$ denotes the vector representation of $NF_{<_0}(h, G)$. Note that we consider all the terms less than or equal to x_0^D instead of *support*$(\bar{g})$. Then, the system (3.1) can be expressed as $AB = C$ with a $D \times D$ matrix A and a $D \times 1$ matrix C. And A is constructed from $[x_0^k]$, $k = 0, \dots, D-1$, and $C = [x_0^D]$.

On the other hand, the system (3.1) coincides with $\phi_p(A)B = \phi_p(C)$ over $GF(p)$ and $\bar{g}$ should be its unique solution because $\bar{H}$ is the reduced Gröbner basis. This means $\det(\phi_p(A)) \neq 0$. Therefore $\det(A) \neq 0$ and the problem $AB = C$ can be uniquely solved and the solution gives the polynomial $g(x_0)$.

LIFTING OF $x_i - \bar{g}_i(x_0)$: For each variable x_i, $1 \leq i \leq n$, we also have a system of linear equation over $\mathbb{Q}[X]/I$ derived from the "shape form", where $b_{k,i}$'s are indeterminates:

$$\sum_{i=0}^{D-1} b_{k,i}[x_0^k] - [x_i] = 0. \tag{3.2}$$

The same argument as in the construction of $g(x_0)$ is applied for each g_i and thus $GB_<(I)$ is the shape basis. □

We note that in the whole computation, the required number of inversion of matrices is one, that is, only the inversion of $\phi_p(A)$ is required.

Next we consider the computation of the RUR.

COROLLARY 3.7. *Assume the same condition as in Proposition 3.6 and let g be the minimal polynomial of x_0 with respect to I. Then, for each x_i, there uniquely exists a univariate polynomial $h_i(x_0)$ such that* $\deg(h_i) < \deg(g)$, $\gcd(g, g')|h_i$, $h_i \in \mathbb{Z}_{<p>}[x_0]$ *and* $g'(x_0)x_i - h_i(x_0) \in I$. *The system of linear equations generated by assigning indeterminates to coefficients of $h_i(x_0)$ has the unique solution over $GF(p)$ and over $\mathbb{Q}$.*

PROOF. Suppose that $\{g(x_0), x_1 - g_1(x_0), \ldots, x_n - g_n(x_0)\}$ is the shape base of I. Then $g'(x_0)x_i - g'(x_0)g_i(x_0)$ belongs to I, which implies the existence of h_i. The uniqueness follows from $\deg(h_i) < \deg(g)$. □

If g is square-free then Corollary 3.7 represents the computation of the RUR by the modular method.

Next we consider the case where g is not square-free. We note that even if g is not square-free, from the square-free decomposition of g and computed h_i's, we can compute the RUR of the radical $\sqrt{I}$ with respect to u by Chinese remainder theorem. Actually it coincides with the definition of the GSL form by Alonso *et al.* (1996). In the following we give a direct method by using Corollary 3.7.

THEOREM 3.8. *Let* $\tilde{H} = \{sq(g)(x_0), \tilde{g}(x_0)x_1 - \tilde{h}_1(x_0), \ldots, \tilde{g}(x_0)x_n - \tilde{h}_n(x_0)\}$, *where* $\tilde{g} = \frac{g'}{\gcd(g,g')}$ *and* $\tilde{h}_i = \frac{h_i}{\gcd(g,g')}$. *Then $\tilde{H}$ is the RUR of $\sqrt{I}$.*

PROOF. We use the same notations as in Corollary 3.7. Note that $h_i = g'g_i \bmod g$ and so $h_i = g'g_i + s_i g$ for some s_i in $\mathbb{Q}[x_0]$, which shows that $\gcd(g, g')$ divides h_i. We show $Id(\tilde{H}) = \sqrt{I}$. As $sq(g) = \frac{g}{\gcd(g,g')}$, $\tilde{g}$ is prime to $sq(g)$ and there is some $f \in \mathbb{Q}[x_0]$ such that $f\tilde{g} \equiv 1 \pmod{sq(g)}$. Then, as $\tilde{h}_i = \frac{g'}{\gcd(g,g')}g_i + \frac{g}{\gcd(g,g')}s_i = \tilde{g}g_i + sq(g)s_i$, we have

$$\begin{aligned} f(x_0)(\tilde{g}(x_0)x_i - \tilde{h}_i(x_0)) &= f(x_0)(\tilde{g}(x_0)x_i - \tilde{g}(x_0)g_i(x_0) - sq(g)(x_0)s_i(x_0)) \\ &\equiv x_i - g_i(x_0) \pmod{sq(g(x_0))}. \end{aligned}$$

As $\sqrt{I} = Id(I \cup \{sq(g(x_0))\})$, the above implies $Id(\tilde{H}) = \sqrt{I}$. □

3.2. General case

Here we consider the case where the modular Gröbner basis is not the shape base. In order to apply the modular method directly, we have to consider the radical of a given ideal I. As our purpose is to obtain a (compact) representation of zeros of the ideal, we may apply ideal decompositions in advance if the computation of the RUR of each component is efficiently done. (González-Vega and Trujillo, 1995; and Rouillier, 1996, also studied this approach).

As a general situation, we may assume that the Gröbner basis G of I with respect to the degree reverse lexical order $<_0$ is given. Then we choose a prime p permissible for $(G, <_0)$. If the Gröbner basis of $Id(\phi_p(G))$ with respect to $<$ is the shape base then we can compute the RUR by the method for shape base case. In the following we treat the cases where it does not hold. In the case, the radical computation by the usual method,

$$\sqrt{I} = Id(I, sq(m_0(x_0)), sq(m_1(x_1)), \ldots, sq(m_n(x_n))),$$

where m_i is the minimal polynomial of x_i with respect to I, (see Becker and Weispfenning, 1993), is very hard even if we apply directly the modular method for change of ordering. Therefore we modify the modular method as follows:

OUTLINE OF GENERAL PROCEDURE

(1) We regard the problem as RUR computations for x_i with respect to x_0 for elimination ideals $I \cap \mathbb{Q}[x_0, x_i]$, $i \leq i \leq n$.
(2) Introducing the ideal quotient computations, the computation is reduced to solving systems of linear equations and we apply the modular method in Section 2.

As a result, a decomposition

$$\sqrt{I} = \cap_{i=1}^{s} \sqrt{J_i},$$

is computed, where each $\sqrt{J_i}$ is co-maximal to other $\sqrt{J_j}$. Instead of the RUR of $\sqrt{I}$, a set of RURs of ideals $\sqrt{J_i}$ is computed. Of course, from those RURs, the RUR of $\sqrt{I}$ can be constructed by Chinese remainder theorem.

Now we show two general procedures for computing the RURs based on the above observation which can also handle the shape base case. These may correspond to algorithms described in Yokoyama *et al.* (1992) which compute shape bases. First we provide the following elementary facts:

LEMMA 3.9. *Let I, J be zero-dimensional ideals of $K[X]$.*

(1) *Suppose that $\sqrt{J} \subset \sqrt{I}$. Then, u is a separating element for I if u is a separating element for J. Especially, if u is a separating element for I, then u is also a separating element for $(I : g)$ for any $g \notin I$.*

(2) *Suppose that $J \subset I$ and f is a polynomial in $K[X]$. Then the minimal polynomial m of f with respect to I is a factor of that with respect to J. Conversely, for each factor g of m, g is the minimal polynomial of f with respect to $(I : \frac{m(f)}{g(f)})$.*

(3) *Suppose that $I = \cap_{i=1}^{s} I_i$ for ideals I_i. If u is a separating element for I, then u is a separating element for every I_i. Conversely, if u is a separating element for every I_i and the minimal polynomial of u with respect to I_i is prime to each other, then u is a separating element for I.*

General procedure without factorization. As we want Gröbner bases of elimination ideals, all the elements of the Gröbner basis are not necessary for each of the following ideal quotients. We compute only the necessary elements by the modular method. (Theorem 2.8 guarantees that the first part of a candidate forms a part of the Gröbner basis, i.e. the Gröbner basis of the elimination ideal.) Thus, we only have to use Gröbner basis G of I and $[x_0^j], [x_0^j x_i]$ which are vector representations of normal forms for solving systems of linear equations.

Let $m_0(x_0)$ be the minimal polynomial of x_0 with respect to I, and $m_0 = \prod_{i=1}^s f_i^{e_i}$ its square free decomposition. Then x_0 is a separating element for $J_k = (I : \frac{m_0(x_0)}{f_k(x_0)})$ and the minimal polynomial of x_0 with respect to J_k is f_k by Lemma 3.9. Moreover, $\sqrt{I} = \cap_{k=1}^s \sqrt{J_k}$ holds, because the set of zeros coincides with each other. Set $C = \{f_1, \dots, f_s\}$. We repeat the following procedure for each x_i, $i = 1, \dots, n$.

For each element f in C, execute the following.

(1) Compute the minimal polynomial $m(x_i)$ of x_i with respect to $J = (I : \frac{m_0(x_0)}{f(x_0)})$ by the modular method.

(2) Compute the minimal polynomial $\tilde{f}(x_0)$ of x_0 with respect to $J' = (J : \frac{m(x_i)}{sq(m(x_i))}) \cap \mathbb{Q}[x_0, x_i] = (I : \frac{m_0(x_0)}{f(x_0)} \frac{m(x_i)}{sq(m(x_i))}) \cap \mathbb{Q}[x_0, x_i]$ by the modular method for ideal quotient.

Then $J' = (J \cap \mathbb{Q}[x_0, x_i] : \frac{m(x_i)}{sq(m(x_i))})$ and the minimal polynomial of x_i with respect to J' is $sq(m(x_i))$ by Lemma 3.9. As the minimal polynomials of variables are square-free, J' is radical (see Becker and Weispfenning, 1993). By Lemma 3.9, $\tilde{f}$ divides f.

(3) If $\tilde{f} = f$ then

$$\sqrt{J} \cap \mathbb{Q}[x_0, x_i] = J',$$

because the set of zeros coincides. In this case, we compute the RUR of J' by ideal quotient $(I \cap \mathbb{Q}[x_0, x_i] : \frac{m_0(x_0)}{f(x_0)} \frac{m(x_i)}{sq(m(x_i))})$.

(4) If $\tilde{f} \neq f$ then $J' \cap \mathbb{Q}[x_0, x_i]$ represents only the zeros (α_0, α_i) of $\sqrt{I} \cap \mathbb{Q}[x_0, x_i]$ such that $\tilde{f}(\alpha_0) = 0$. In this case, we compute the RUR of $Id(J \cup \{\tilde{f}(x_0)\})$ by ideal quotient $(I \cap \mathbb{Q}[x_0, x_i] : \frac{m_0(x_0)}{\tilde{f}(x_0)} \frac{m(x_i)}{sq(m(x_i))})$.

Then C is replaced with $\{\tilde{f}, f/\tilde{f}\} \cup (C \setminus \{f\})$ and apply the procedure also for $f/\tilde{f}$. If the RUR of $\sqrt{J} \cap \mathbb{Q}[x_0, x_j]$ is already computed for another x_j, it should be slightly modified as follows.

$$f'(x_0)x_j - h_j(x_0) \to (\tilde{f})'(x_0)x_j - \tilde{h}_j(x_0),$$

where $h_j \equiv \tilde{h}_j \frac{f}{\tilde{f}} \pmod{\tilde{f}}$. See the next subsection for the detail.

After processing all elements in C, C is reconstructed so that it consists of factors of the minimal polynomial appeared in the procedure. That is, we have $C = \{\tilde{f}_1, \dots, \tilde{f}_t\}$, where $sq(m_0) = \prod_{i=1}^t \tilde{f}_i$, and the RUR of $Id(\sqrt{I} \cup \{\tilde{f}_i(x_0)\})$ is computed for every $\tilde{f}_i$.

General procedure with factorization. If we use the complete factorization of $m_0(x_0)$, the computed results correspond to the prime divisors of I. In this case, C consists of all irreducible factors of $m_0(x_0)$. And the result gives the prime decomposition of $\sqrt{I}$.

LEMMA 3.10. *For each f in C, $J_0 = Id(\sqrt{I} \cup \{f(x_0)\}) = (\sqrt{I} : \frac{sq(m_0(x_0))}{f(x_0)})$ is a maximal ideal and $J = (I : \frac{m_0(x_0)}{f(x_0)^e})$ is its associated primary ideal, where e is the multiplicity of f as a factor of m_0.*

PROOF. As x_0 is a separating element, $\sqrt{I}$ has the shape base with respect to $<$ and so $\sqrt{I} = Id(sq(m_0(x_0)), x_1 - g_1(x_0), \ldots, x_n - g_n(x_0))$ for some univariate polynomials $g_1, \ldots, g_n$. Then the minimal polynomial of x_0 with respect to J_0 is f which is irreducible over $\mathbb{Q}$. This implies that J_0 is a maximal ideal. Comparing the zeros of J_0 and those of J, J is a primary ideal associated with J_0. □

As J_0 is maximal, the minimal polynomial $m^*(x_i)$ of x_i with respect to J_0 is irreducible over $\mathbb{Q}$ and the minimal polynomial $m(x_i)$ of x_i with respect to J coincides with m^* or its power. Then $J' = (J : \frac{m(x_i)}{m^*(x_i)})$ is also a primary ideal associated with J_0 and the minimal polynomial $\tilde{f}$ of x_0 with respect to J' coincides with f, which implies that the set C is never reconstructed.

3.3. COMPUTATION OF PRIME DIVISORS

Here, we give a method to compute prime components of a given ideal from its RUR. Suppose that the following RUR is already computed:

$$J = \sqrt{I} = Id(g(x_0), g'(x_0)x_1 - h_1(x_0), \ldots, g'(x_0)x_n - h_n(x_0)),$$

where $g(x_0)$ is square-free and $g = \prod f_i$ is the irreducible factorization of g over $\mathbb{Q}$. Then J is decomposed into prime components as follows.

$$J = \cap J_i; \qquad J_i = J + Id(f_i(x_0)) = \left(J : \frac{g(x_0)}{f_i(x_0)}\right).$$

From $J_i = J + Id(f_i(x_0))$, we have

$$J_i = Id(f_i, (g' \bmod f_i)x_1 - (h_1 \bmod f_i), \ldots, (g' \bmod f_i)x_n - (h_n \bmod f_i)).$$

In general, however, $g'(x_0) \bmod f_i(x_0)$, $h_i(x_0) \bmod f_i(x_0)$ tend to have large coefficients, which will make the subsequent computation hard.

On the other hand, each J_i also has the following RUR form.

$$J_i = Id(f_i(x_0), f_i'(x_0)x_1 - h_{1,i}(x_0), \ldots, f_i'(x_0)x_n - h_{n,i}(x_0)).$$

By using $J_i = (J : \frac{g(x_0)}{f_i(x_0)})$ we can show

$$h_j \equiv h_{j,i}\frac{g}{f_i} \qquad (\bmod f_i).$$

By the above equation, $h_{j,i}$ is computed from h_j, f_i and g and the computation can be done efficiently by the modular method. By applying Hensel lifting for this computation, the execution time is expected to be short if $h_{j,i}$ has small coefficients.

REMARK 3.11. If we compute the inverse of $\frac{g}{f_i}$ modulo f_i then the computation of $h_{j,i}$ is reduced to a multiplication and a residue computation. This inverse, however, tends to have huge coefficients in general and it does not seem practical.

4. Finding Separating Elements

Here we give a brief discussion on finding separating elements. As mentioned in Remark 3.5, it is desirable to find a separating element from variables. But, if there is no such a variable, we have to find a separating element from linear sums of variables.

Let I be a zero-dimensional ideal in $\mathbb{Q}[X]$, where $X = \{x_1, \ldots, x_n\}$, G its Gröbner basis with respect to a fixed order $<$ and $D = \dim_{\mathbb{Q}}(\mathbb{Q}[X]/I)$. It is well known that there are separating elements among linear sum of variables $a_1x_1 + \cdots + a_nx_n$. By Yokoyama *et al.* (1992), there exists a separating element in the set constructed from a maximally independent set/n-base set of $nD^2 + 1$ elements. See Lemma 4.4 for the detail.

Definition 4.1. (Yokoyama *et al.*, 1989 and Zippel, 1990) *Let S be a subset of K^n. S is called a maximally independent (an n-base) set over K, if any distinct n elements of S are linearly independent over K.*

We can construct a maximally independent set over $\mathbb{Q}$ with any cardinality in terms of integer parameters. For example, $S = \{(1, u, u^2, ..., u^{n-1})|u \in \mathbb{Z}\}$ is a maximally independent set with infinitely many elements. In fact, Rouillier (1996, 1997) used this set for generating candidates of a separating element (see Yokoyama *et al.*, 1989; Zippel, 1990, for other examples).

On the other hand, for a randomly generated linear sum u of variables, the possibility that u is a separating element is very high. So it will be practical to compute the RUR for an element u without guaranteeing that u is a separating element and to check the correctness of the computed result. But, in unlucky cases, the above approach needs recomputations certain times and it becomes far from practical. Thus, to handle such cases, we introduce efficiently computable tests whether u is a separating element in before hand. The efficiency of tests is derived from the use of modular computation. Rouillier (1996, 1997) also used modular computations for the test of a separating element (see the discussion in Section 6).

4.1. Quick Modular Test for Shape Base Case

Let p be a permissible prime for $(G, <)$, u a candidate of a separating element and $m_{p,u}$ the minimal polynomial of $\phi_p(u)$ with respect to $Id(\phi_p(G))$. If $deg(m_{p,u}) = D$ then $Id(\phi_p(G)) + Id(z - \phi_p(u))$ has the shape base with respect to the newly introduced variable z. Then $I + Id(z - u)$ has the shape base with respect to z by Theorem 3.6. If there exists an element such that the degree of its minimal polynomial with respect to I is D, then we can expect that $deg(m_{p,u}) = D$ with a high probability, for a linear sum u of variables and a permissible prime p randomly chosen. Thus we have the following quick modular test for shape base case.

Quick test

```
Step 1. Provide several primes permissible for $(G, <)$.
Step 2. For each prime $p$, do the following:
          Compute the minimal polynomial $m_{p,u}$ of $\phi_p(u)$.
          If deg($m_{p,u}$) = $D$, then $I + Id(z - u)$ has the shape base
          with respect to the newly introduced variable $z$.
          (This means that $z$ is a separating element in $I + Id(z - u)$,
          or equivalently $u$ is a separating element in $I$.)
```

Once we know that I has a shape base, we may search for another u with smaller coefficients because the cost for linear equation solving depends on the size of coefficients in $NF(u^i, G)$ $(i = 0, \dots, D)$.

4.2. GENERAL MODULAR TEST

Next we consider a general test which can handle I which may not have a shape base by using the modular technique. First we provide "radical compatibility" of primes.

DEFINITION 4.2. Let $m_1, \dots, m_n$ be the minimal polynomials of variables $x_1, \dots, x_n$, respectively. A prime p is *radical compatible* with I if p is compatible with I, every m_i belongs to $\mathbb{Z}_{<p>}[X]$ and $\phi_p(sq(m_i))$ is square-free.

We note that if p is permissible with $(G, <)$, then p is compatible with I and every m_i belongs to $\mathbb{Z}_{<p>}[X]$.

LEMMA 4.3. *Suppose that p is radical compatible with I. Then, $\phi_p(\sqrt{I} \cap \mathbb{Z}_{<p>}[X])$ is radical. Moreover, if $\phi_p(u)$ is a separating element of $\phi_p(I \cap \mathbb{Z}_{<p>}[X])$, then u is a separating element.*

From Yokoyama *et al.* (1992), we have the guarantee of the existence of separating element and a bound of the number of trials for finding a separating element from candidates.

LEMMA 4.4. *If $p > nED + 1$, where E is the number of prime divisors of I, there is a separating element for $Id(\phi_p(G))$ among all linear sums of variables over $GF(p)$. Moreover, there is a separating element among $nED + 1$ linear sums which correspond to a maximally independent set.*

As $E \leq D$, Lemma 4.4 holds for $p > nD^2 + 1$. Then we have

PROPOSITION 4.5. (1) *In the radical case, if p is radical compatible and $p > nD^2 + 1$ and the candidates of separating elements are constructed from a maximally independent set with $nD^2 + 1$ elements,* QUICK TEST *with the fixed prime p can find a separating element after executing at most $nD^2 + 1$ minimal polynomial computations.*

(2) *In non-radical cases, a separating element is found as an element whose minimal polynomial has the maximal degree square-free part. For such cases a separating element can be found by checking all the $nD^2 + 1$ candidates.*

The criterion in Proposition 4.5 (2) is very simple and gives a good worst case complexity for a non-radical case. However, it does not seem quite practical. Thus, aiming to obtain a practical method, we propose the following strategy.

Here, we assume that the minimal polynomials m_i are already computed (by the modular method) and a prime p is chosen so that p is permissible with $(G, <)$, p is radical compatible with I and $p > nD^2 + 1$. Let $\bar{u}$ be a candidate of a separating element for $Id(\phi_p(G))$.

General strategy for finding separating elements

Step 1. Compute a non-trivial ideal decomposition:

$$\bar{J} = \cap_{i=1}^{s} \bar{J}_i,$$

where $\bar{J}$ is an ideal of $GF(p)[X]$ obtained by a number of the ideal operations, adding certain polynomials or ideal quotient, and $\sqrt{\bar{J}}=\sqrt{Id(\phi_p(G))}$.

Step 2. Test whether $\bar{u}$ is a separating element for every $\bar{J}_i$ and whether the minimal polynomial of $\bar{u}$ with respect to $\bar{J}_i$ is prime to each other.
If so, $\bar{u}$ is a separating element for $Id(\phi_p(G))$.

The general strategy reduces the problem, finding a separating element for $Id(\phi_p(G))$, to a number of much smaller problem, finding a separating element for each $\bar{J}_i$. However, as additional computation is required for getting non-trivial decomposition, there is a trade-off between the reduction and the decomposition. But it seems easy to decompose a zero-dimensional ideal over a finite field, due to efficient factorizations and no coefficient growth in Gröbner bases computation, and this fact supports the general strategy.

5. Experiment

5.1. Computation of the RUR of the radical

We implement the new method for shape base case on a computer algebra system `Risa/Asir` (Noro and Takeshima, 1992) and measure the timings. Quick test in Section 4.1 provides us an efficient method to detect a given ideal having a shape base. In the experiment we use well-known benchmark problems, each of which is known to have a shape base by Quick test. As a *reference* we also show the timings for Rouillier's method on the *RealSolving servers*, `ServerRS` and `serveur_rsdemo` (see Rouillier, 1998). `ServerRS` has a general function to search for a separating element. On the other hand our current implementation only deals with shape base cases. Since the separating element search in a general case requires various additional costs, it is difficult to compare two methods directly. But the result shows a certain quality of the new method and its implementation.

The measurement is made on a PC (300MHz Pentium II, 512MB of memory). Timings are given in seconds.

$C(n)$ The cyclic n-roots system of n variables. (Faugère *et al.*, 1993).
$\{f_1,\ldots,f_n\}$ where $f_k = \sum_{i=1}^{n} \prod_{j=i}^{k+j-1} c_{j \bmod n} - \delta_{k,n}$. ($\delta$ is the Kronecker symbol.)
The variables and ordering : $c_n \succ c_{n-1} \succ \cdots \succ c_1$

$K(n)$ The Katsura system of n+1 variables.
$\{u_l - \sum_{i=-n}^{n} u_i u_{l-i} (l = 0,\ldots,n-1), \sum_{l=-n}^{n} u_l - 1\}$
The variables and ordering : $u_0 \succ u_1 \succ \cdots \succ u_n$.
Conditions : $u_{-l} = u_l$ and $u_l = 0(|l| > n)$.

$R(n)$ e7 in Rouillier (1996).
$\{-1/2 + \sum_{i=1}^{n} (-1)^{i+1} x_i^k (k = 2,\ldots,n+1)\}$
The variables and ordering : $x_n \succ x_{n-1} \succ \cdots \succ x_1$.

$D(3)$ e8 in Rouillier (1996).
The variables and ordering : $b \succ a \succ s \succ v \succ u \succ t \succ z \succ y$.

Table 1. Statistics of the input ideals.

	$K(5)$	$K(6)$	$K(7)$	$K(8)$	$C(6)$	$C(7)$	$R(5)$	$R(6)$	$D(3)$
DIM	32	64	128	256	156	924	144	576	128
DRL	0.8	7.2	68	798	3.1	1616	11	1775	30

DIM : the $\mathbb{Q}$-dimension of the residue class ring R/I.

DRL : the time to compute the degree reverse lex Gröbner basis on `Asir`.

Table 2. Execution time on `Asir` (s).

	$K(6)$	$K(7)$	$K(8)$	$C(6)$	$C(7)$	$R(5)$	$R(6)$	$D(3)$
Total	7.4	69	1209	4.6	1643	52	8768	67
Modular	0.4	3.2	26	0.5	57	6.5	384	3.1
Table	1.1	12	308	1.4	762	15	2861	7.3
Equation	4.1	43	775	1.4	641	22	3841	45
GC	1.7	10	100	1.2	181	7.8	1681	11

Modular : Quick test (Modular Gröbner basis computation).

Table : Normal form computation.

Equation : Solving systems of linear equations.

GC : Garbage collection time.

Table 3. Number of normal form computation in the new method.

$K(6)$	$K(7)$	$K(8)$	$C(6)$	$C(7)$	$R(5)$	$R(6)$	$D(3)$
20+71	35+136	70+265	156+163	924+932	144+160	576+583	128+136

'n+m' : n = the number of normal form computation in Step 1;
m = the number of normal form computation in Step 2;
where Step 1 and Step 2 are explained in Section 6.

The following polynomials are added so that a newly introduced variable w is a separating element for each system. In order to equalize the condition for computing the RUR on `Asir` and the RealSolving servers we set the order of w as the highest one among the variables when we compute the degree reverse lex Gröbner basis for each example. This implies that the QUICK TEST in `Asir` and SEPARATING ELEMENT SEARCH in the RealSolving servers are done only once on all the systems.

In Tables 1–3 we refer to each augmented system by the same name.

$C(6)$	$w-(c_1+3c_2+9c_3+27c_4+81c_5+243c_6)$
$C(7)$	$w-(c_1+3c_2+9c_3+27c_4+81c_5+243c_6+729c_7)$
$K(n)$	$w-u_n$
$R(5)$	$w-(x_1-3x_2-2x_3+3x_4+2x_5)$
$R(6)$	$w-(x_1-3x_2-2x_3+3x_4+2x_5-4x_6)$
$D(3)$	$w-y$

5.2. PRIME DECOMPOSITION

We compute the prime decomposition of $C(7)$. Here we use $w-(c_1+2c_2-6c_3+4c_4-10c_5+6c_6-9c_7)$ as a polynomial added to $C(7)$. Then we compute the RUR with respect to w. Let $f_0(w)$ be the minimal polynomial of w. Then $\deg_w f_0 = 924$ and it takes 1470 s to factorize $f_0(w)$. $f_0(w)$ has 91 irreducible factors; 21 factors of degree 24, 14 factors of

Table 4. Execution time on the RealSolving servers (s).

		$K(6)$	$K(7)$	$K(8)$	$C(6)$	$C(7)$	$R(5)$	$R(6)$	$D(3)$
serveur_rsdemo	Total	7.8	89	1705	8.3	4552	33	7047	57
	Search	0.8	8.6	104	2.6	850	5.7	603	5.7
	Table	4	62	1114	3.9	1518	18	2931	21
	RUR	3	18	487	1.8	2184	8.9	3513	30
ServerRS	Total	12.6	191	3487	19.5	—	80	—	74
	Table	9.3	156	2779	14.3	—	53	—	54
	RUR	3.3	35	708	5.2	—	28	—	20

Table : Normal form computation.
RUR : RUR computation by symmetric function method.
Search : Separating element search.
— : Memory exhaustion.

degree 12, 35 factors of degree 6 and 21 factors of degree 2. For each factor we compute the simplified form of the RUR by the method in Section 3.1 and it takes 693 s.

6. Discussion

In the following the word *field operation* means arithmetic operation on the base field $\mathbb{Q}$, and the word *machine operation* means arithmetic operation on machine words.

6.1. Complexity

Here we give a rough estimation on the complexity of the RUR computation of an ideal I for *shape base case* after finding a separating element, because this case is a typical one for demonstrating the effect of the modular technique employed here. Let $D = \dim_{\mathbb{Q}}(\mathbb{Q}[X]/I)$, where $X = \{x_0, \ldots, x_n\}$, x_0 is known as a separating element, and $\{w_j\}$ the $\mathbb{Q}$-linear monomial base of $\mathbb{Q}[X]/I$ corresponding to the Gröbner basis G of I. The new method proposed here consists of the following steps.

Outline of new method

Step 1. Computation of the multiplication map $M_{x_0,I}$ with respect to the $\mathbb{Q}$-linear base $\{w_j\}$. (See Definition 3.1.)

Step 2. Computation of the normal forms of x_0^i, $i = 0, \ldots, D$, from the result of Step 1.

Step 3. Computation of the minimal polynomial of x_0 by solving a system of linear equations with Hensel lifting (Algorithm 2.12).

Step 4. Computation of the RUR by solving systems of linear equations with Hensel lifting.

The whole computation is divided into two parts, normal form computations (Step 1,2) and solving systems of linear equations (Step 3,4). Here we call the part of normal form computations *the step of making tables.*

(A) Though Step 1 consists of at most D normal form computations, it is hard to estimate directly the number of required field operations. So we obey the estimate for computing multiplication maps for all the variables by Rouillier (1996), which is $O(nD^3)$. Step 2 contains D normal form computations, each of which is done by a multiplication of $D \times D$ matrix and a vector. Step 2 requires $O(D^3)$ steps. Thus we have

PROPOSITION 6.1. *Step 1 and Step 2 require $O(nD^3)$ field operations.*

(B) Next we estimate the cost for solving systems of linear equations, where the modular technique is employed and its effect can be seen in the experiments in the previous section. As this is the dominant part in the new method and the termination is dependent on the size of the RUR, we give its complexity in terms of machine operation. The estimation on the complexity given in the below also supports its efficiency *in theory.* Here M_R denotes the maximal value of $mag(g)$ among all elements g of the RUR, and M denotes $mag(A)$, where A is the matrix constructed from $[x_0^i]$'s and $mag(A)$, $mag(g)$ is the maximal value of the sum of word sizes of the numerator and denominator of each entry of A, or each coefficient of g respectively.

PROPOSITION 6.2. *The number of machine operations required for Step 3,4 is as follows.*

$$cD^3 + nM_RMD^2 + MD^2 + nMD,$$

We remark that $M_R < M$ often holds, and for such a case the total cost is bounded by $cD^3 + nM^2D^2 + MD^2 + nMD$.

PROOF. We give an outline of the proof. Let $AB = C$ be the equation to be solved for B and let B_0 be its unique solution over $\mathbb{Q}$. (A is a $D \times D$ matrix.) We set $M = max(mag(A), mag(C))$. Then the complexity is estimated as follows under the assumption that p is a single word integer.

(1) The computations of $\phi_p(A)$ and $\phi_p(C)$ require MD^2 and MD machine operations over $GF(p)$, respectively.
(2) The inversion of $D \times D$-matrix $\phi_p(A)$ requires cD^3 machine operations over $GF(p)$, where c is a small constant.
(3) The Hensel lifting requires $mag(B_0)MD^2$ machine operations.

We have the proposition by gathering each part. □

6.2. CHARACTERIZATION OF THE NEW METHOD

(a) USE OF MINIMAL POLYNOMIAL

The new method is based on the computation of the minimal polynomial of a linear map, whereas Rouillier's method is based on the computation of the characteristic polynomial of a linear map. We can compute the minimal polynomial as a solution of a linear equation, which enables us to use modular methods. In general it is difficult to handle the characteristic polynomial in a similar way, but in shape base case the minimal polynomial coincides with the characteristic polynomial and we can compute the characteristic polynomial by modular methods. In general case we have to consider the characteristic polynomial or the radical computation because of the existence of multiplicities. In the new method we propose to use ideal quotient computations instead, which allow again an application of the modular method.

(b) USE OF MODULAR METHODS

The new method uses modular methods in various purposes:

(1) quick test for shape base case,

(2) separating element search by modular ideal decomposition,
(3) guess of the form of the result,
(4) linear equation solving by Hensel lifting.

These are all based on the notion of (radical) compatibility of a prime. Under the compatibility the existence of a solution implies the correctness of the solution.
As for (3) we apply the method in Section 2.2. If the guessed form is sparse, the size of the resulting linear equation becomes small. For $C(7)$ the dimension of the residue class ring is 924. But the size of the matrix constructed from the modular RUR is 132×132, which makes the linear equation solving efficient.

(c) Complexity

In shape base case, the experiment and the complexity analysis show that the new method can compute the RUR with smaller cost (cf. Rouillier, 1996). This is a benefit of the special method applicable to shape base case.
When the given ideal does not have a shape base, it is difficult to analyze the complexity. As for the step of making tables, the number of normal form computations is $O(nD)$ in the new method. But, the new method requires additional computations, the amount of which shall depend on the shape of the ideal, i.e. the number of primary components and so on. Therefore, to discuss the practical efficiency, we need precise experiments, which will be done in our future study.

(d) Separating element search

In general situation, we proposed a method to find a separating element based on the radical compatibility of a prime and modular ideal decomposition. We can also apply the techniques, candidates from a maximally independent set and guess by modular computation. Rouillier (1996, 1997), in fact, proposed a modular method based on a maximally independent set. These must contribute theoretical efficiency, however, they seem to disturb the practically efficiency. So, from the practical point of view, both methods should be implemented for aiming probabilistic efficiency.

6.3. Future works

Besides the full implementation of the new method there still remain the following.

Chinese remainder theorem approach

We can compute a candidate of the RUR by *Chinese remainder theorem (CRT)*. FGLM algorithm (Faugère *et al.*, 1993) on a finite field requires $O(nD^3)$ steps and it is often easy to compute such a candidate by using FGLM and CRT for small D. However, the correctness check of the candidate requires normal form computations for each element of the candidate, and it will be necessary to prepare the same normal form table as used in the new method for an efficient check. A detailed comparison between the method proposed here and methods based on CRT should be done in our next study.

Parallel computation

In the method proposed here, there are several parts which can be parallelized; each linear equation solving, combination of Hensel lifting and CRT, and normal form computation of $\{x_0^i\}$ from the multiplication map of x_0^k for some fixed k. Among those points, the first one has already been realized for UNIX workstation cluster. The others seem easily realizable, but various techniques should be required for an efficient implementation.

Further improvements

We list remaining problems which will be studied in our future work.

- Improvement of solving systems of linear equations.
- Extension to systems with rational function coefficient using polynomial-rational function conversion.
- Efficient finding of a *small* separating element.
- Incremental decomposition using non-separating elements.
- Combination with methods based on CRT.

References

Alonso, M.-E., Becker, E., Roy, M.-F., Wörmann, T. (1996). Zeros, multiplicities and idempotents for zero dimensional systems. In González-Vega, L. *et al.*, eds, *Algorithms in Algebraic Geometry and Applications*, pp. 1–16. Basel, Birkhaüser.

Becker, E., Marinari, M. G., Mora, T., Traverso, C. (1994). The shape of the Shape Lemma. In *Proceedings of the ISSAC'94*, pp. 129–133. New York, ACM Press.

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

Buchberger, B. (1965). Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. Ph.D. Thesis, Mathematical Institute of the University of Innsbruck, Austria.

Buchberger, B. (1970). Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleischunssystem. *Aeq. Math.*, **4**, 374–383.

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

Gianni, P., Mora, T. (1989). Algebraic solution of systems of polynomial equations using Gröbner bases. In *Proceedings of the AAECC-5*, LNCS **356**, pp. 247–257. Springer.

Gonzâlez-Vega, L., Trujillo, G. (1995). Using symmetric functions to describe the solution set of a zero dimensional ideal. In *Proceedings of the AAECC-11*, LNCS **948**, pp. 232–247. Springer.

Gräbe, H.-G. (1993). On lucky primes, *J. Symb. Comput.*, **15**, 199–209.

Kobayashi, H., Moritsugu, S., Hogan, R. W. (1988). On solving systems of algebraic equations. In *Proceedings of the ISSAC'88*, LNCS **358**, pp. 139–149. Springer.

Lakshman, Y. N. (1990). On the complexity of computing Gröbner bases for zero-dimensional polynomial ideals. Ph.D. Thesis, Rensselaer Polytechnic Institute, U.S.A.

Noro, M., Takeshima, T. (1992). Risa/Asir—a computer algebra system. In *Proceedings of the ISSAC'92*, pp. 387–396. New York, ACM Press. Binaries for various platforms are available from `ftp://endeavor.fujitsu.co.jp/ pub/isis/asir`.

Noro, M., Yokoyama, K. (1995). New methods for the change of ordering in Gröbner basis computation. FUJITSU ISIS Research Report ISIS-RR-95-8E. This is available at `ftp://endeavor.fujitsu.co.jp/pub/isis/asir/paper/changeoforder.ps.gz`.

Rouillier, F. (1996). Résolution des systèmes zéro-dimensionnels. Ph.D. Thesis, University of Rennes I, France.

Rouillier, F. (1997). The rational univariate representation. Preprint (English version).

Rouillier, F. (1998). RealSolving Servers `ServerRS` and `serveur_rsdemo`. Binaries for various platforms are available from `http://www.loria.fr/~rouillie`.

Yokoyama, K., Noro, M., Takeshima, T. (1989). Computing primitive elements of extension fields. *J. Symb. Comput.*, **8**, 553–580.

Yokoyama, K., Noro, M., Takeshima, T. (1992). Solution of systems of algebraic equations and linear maps on residue class rings. *J. Symb. Comput.*, **14**, 399–417.

Wang, P. S., Guy, J. T., Davenport, J. H. (1982). p-adic reconstruction of rational numbers. *SIGSAM Bull.*, **16**, 2–3.

Zippel, R. (1990). Interpolating polynomials from their values. *J. Symb. Comput.*, **9**, 375–403.