J. Symbolic Computation (1989) **8**, 545–552

On Radical Zero-Dimensional Ideals

HIDETSUNE KOBAYASHI,* SHUICHI MORITSUGU† AND ROBERT W. HOGAN‡

* *Department of Mathematics, College of Science and Technology, Nihon University, Chiyoda-ku, Tokyo* 101, *Japan*
† *Department of Information Science, Faculty of Science, University of Tokyo, Bunkyo-ku, Tokyo* 113, *Japan*
‡ *Citizen Watch Co. Ltd., Tokorozawa-shi, Saitama* 359, *Japan*

(*Received* 24 *November* 1987)

This paper shows an algorithm to construct the Gröbner bases of radicals of zero-dimensional ideals. Computing radicals is equivalent to solving systems of algebraic equations without counting the multiplicities of solutions. We prove that the Gröbner basis of a radical zero-dimensional ideal takes a special form after a suitable transformation of coordinates.

1. Introduction

To solve a simultaneous system of algebraic equations, one may employ either the classical method of general elimination of variables (van der Waerden, 1931) or elimination methods proposed by Trinks (1978) and Buchberger (1970). Trinks's method entails computing a Gröbner basis with lexicographic ordering to obtain a polynomial in one variable. In practice this technique is only suitable for small-sized problems. Buchberger's method is to compute a Gröbner basis with total degree ordering and extract a polynomial in a single variable. Each root of this polynomial is subsequently substituted in each member of the Gröbner basis and once again a Gröbner basis is computed, but it is difficult to maintain numerical accuracy in this process.

One of the authors (S.M.) has observed, through actually solving numerous systems of algebraic equations, that the lexicographic order Gröbner basis often takes a particular form, which is similar to the observation of Trinks (1984). Consider the following system of algebraic equations:

$$\left.\begin{array}{c} f_1(x_1, x_2, \ldots, x_n) = 0 \\ f_2(x_1, x_2, \ldots, x_n) = 0 \\ \vdots \\ f_m(x_1, x_2, \ldots, x_n) = 0 \end{array}\right\} \tag{1.1}$$

When this system of equations possesses finitely many common solutions, in virtually all cases the lexicographic order Gröbner basis for I, the ideal generated by $f_1, f_2, \ldots, f_m$, will take the following form

$$\left.\begin{array}{c} x_1 - F_1(x_n) \\ x_2 - F_2(x_n) \\ \vdots \\ x_{n-1} - F_{n-1}(x_n) \\ F_n(x_n) \end{array}\right\} \tag{1.2}$$

0747–7171/89/120545+08 $03.00/0

In other words, for almost any given system of algebraic equations, computing the common roots of the system (1.1) is equivalent to computing the common roots of the system (1.2) for some appropriate polynomials $F_1, F_2, \ldots, F_n$. However, this property does not hold in all cases. We may explicitly demonstrate several instances in which the property does not hold.

In section 2 of this paper we will prove that when the ideal I is zero-dimensional and radical (i.e. $\sqrt{I} = I$), after a possible transformation of coordinates, the lexicographic order Gröbner basis of I takes the form given in eqn (1.2). Even if I fails to be radical, since $\sqrt{\sqrt{I}} = \sqrt{I}$, by computing the radical of I we may obtain a Gröbner basis of the form given in eqn (1.2). We will present a method to compute the radical of an arbitrary zero-dimensional ideal employing the method of primary decomposition proposed by Gianni *et al.* (1988) in section 3. Since the set of zeros of $\sqrt{I}$ is the same as the set of zeros of I, the algorithm proposed in Kobayashi *et al.* (1988) allows us to compute the common zeros of ideal I in an efficient fashion.

In this paper, we assume that the polynomials are in a ring $\mathbf{Q}[x_1, x_2, \ldots, x_n]$ with $\mathbf{Q}$ the field of rational numbers, and that the variable ordering is $x_1 > x_2 > \ldots > x_n$, $z_1 > z_2 > \ldots > z_n$, unless we specify otherwise. We also assume that all Gröbner bases which appear in this paper are lexicographic order and reduced as defined in Buchberger (1985), which we follow for other basic notation and definitions.

2. Gröbner basis of $\sqrt{I}$

Let I be an ideal in $\mathbf{Q}[x_1, x_2, \ldots, x_n]$ such that $\sqrt{I} = I$. Then there are a finite number of prime ideals $p_1, p_2, \ldots, p_s$ such that $I = p_1 \cap p_2 \cap \ldots \cap p_s$.

PROPOSITION 2.1. *Let p be a zero-dimensional prime ideal in $\mathbf{Q}[x_1, x_2, \ldots, x_n]$. For almost all linear coordinate transformations, the Gröbner basis of p with respect to the new coordinates $z_1, z_2, \ldots, z_n$ is of the form*

$$\{z_1 - \varphi_1(z_n), z_2 - \varphi_2(z_n), \ldots, z_{n-1} - \varphi_{n-1}(z_n), \varphi_n(z_n)\},$$

for some $\varphi_j(z_n) \in \mathbf{Q}[z_n]$. □

Gröbner (1949) discussed the basis of zero-dimensional prime ideals like this form. However, this is easy to see from Proposition 7.1 of Gianni *et al.* (1988), together with the definition of reduced Gröbner bases.

PROPOSITION 2.2. *Let I be a zero-dimensional ideal with $\sqrt{I} = I$. Then, for almost all linear coordinate transformations, the Gröbner basis of I with respect to the new coordinates $z_1, z_2, \ldots, z_n$ has the form*

$$\{z_1 - h_1(z_n), z_2 - h_2(z_n), \ldots, z_{n-1} - h_{n-1}(z_n), h_n(z_n)\},$$

for some $h_j(z_n) \in \mathbf{Q}[z_n]$. □

PROOF.
Step 1. I may be represented as an intersection of prime ideals $p_1, p_2, \ldots, p_s$ ($p_i \neq p_j$ for $i \neq j$). After a suitable coordinate transformation, the Gröbner basis of each prime ideal p_i takes the form

$$\{z_1 - F_{1,i}(z_n), z_2 - F_{2,i}(z_n), \ldots, z_{n-1} - F_{n-1,i}(z_n), F_{n,i}(z_n)\}.$$

Since p_i is zero-dimensional, $F_{n,i}(z_n) \neq 0$. When we consider two prime ideals p_1 and p_2, then we have two cases:

$$\begin{cases} \text{case 1} & F_{n,1} = F_{n,2}, \\ \text{case 2} & F_{n,1} \neq F_{n,2}. \end{cases}$$

In case 1, since $p_1 \neq p_2$, there exists an integer j such that $F_{j,1} \neq F_{j,2} (\mathrm{mod}\ F_{n,1})$. Hence we have (at least) two zeros of $p_1 \cap p_2$ whose coordinates are $(\ldots, F_{j,1}(\alpha), \ldots, \alpha)$ and $(\ldots, F_{j,2}(\alpha), \ldots, \alpha)$ respectively, where α is a root of $F_{n,1}$. By a suitable linear coordinate transformation, no two zeros of $p_1 \cap p_2$ have the same nth coordinate (Fig. 1).

This implies that case 1 will not happen after a suitable coordinate transformation. Therefore, we have only to consider case 2. In this case, since $F_{n,1} \neq F_{n,2}$, these two polynomials are relatively prime. Thus, we have two polynomials A and B in $\mathbf{Q}[z_n]$ such that $A \cdot F_{n,1} + B \cdot F_{n,2} = 1$. Since $A \cdot F_{n,1}$ (respectively $B \cdot F_{n,2}$) is contained in p_1 (respectively p_2), we have $p_1 + p_2 = (1)$, and from this equation we have $p_1 \cap p_2 = p_1 p_2$. The ideal $p_1 p_2$ is generated by:

$$\{(z_i - F_{i,1}(z_n)) \cdot (z_j - F_{j,2}(z_n))\}_{1 \leq i,j \leq n-1} \cup \{F_{n,1}(z_n) \cdot (z_j - F_{j,2}(z_n))\}_{1 \leq j \leq n-1}$$
$$\cup \{F_{n,2}(z_n) \cdot (z_i - F_{i,1}(z_n))\}_{1 \leq i \leq n-1} \cup \{F_{n,1}(z_n) \cdot F_{n,2}(z_n)\}.$$

We note that

$$A \cdot F_{n,1}(z_n) \cdot (z_j - F_{j,2}(z_n)) + B \cdot F_{n,2}(z_n) \cdot (z_j - F_{j,1}(z_n)) = z_j - A \cdot F_{n,1} \cdot F_{j,2} - B \cdot F_{n,2} \cdot F_{j,1}$$

is contained in $p_1 \cap p_2$.

Step 2. Now we prove that

$$G = \{z_j - A \cdot F_{n,1} \cdot F_{j,2} - B \cdot F_{n,2} \cdot F_{j,1}, \quad F_{n,1} \cdot F_{n,2}\}_{1 \leq j \leq n-1}$$

is the Gröbner basis for the ideal $p_1 \cap p_2$.

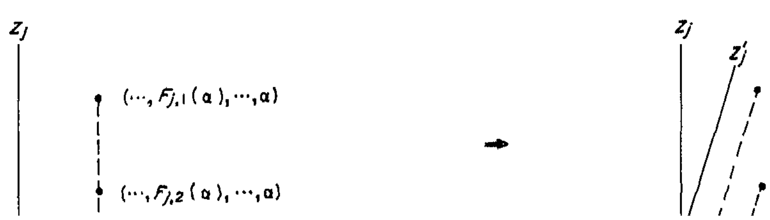
Let f be any element of $p_1 \cap p_2$, then f can be reduced to

$$f(A \cdot F_{n,1} \cdot F_{1,2} + B \cdot F_{n,2} \cdot F_{1,1}, \ldots, A \cdot F_{n,1} \cdot F_{n-1,2} + B \cdot F_{n,2} \cdot F_{n-1,1}, z_n),$$

which we denote by $\bar{f}(z_n)$. Since

$$\bar{f}(z_n) \in p_1 \cap p_2, F_{n,1}(z_n) | \bar{f}(z_n) \quad \text{and} \quad F_{n,2}(z_n) | \bar{f}(z_n)$$

and so $F_{n,1} \cdot F_{n,2} | \bar{f}(z_n), \bar{f}(z_n)$ can be reduced to 0 by $F_{n,1} \cdot F_{n,2}$. Thus, any element of $p_1 \cap p_2$ can be reduced to 0 by G, and it is easy to see that the S polynomial of each pair is reduced to 0. This shows that G is the Gröbner basis.



Step 3. Suppose that the Gröbner basis of $p_1 \cap p_2 \cap \ldots p_i$ $(i < s)$ has the form:

$$\{z_1 - H_1(z_n), \ldots, z_{n-1} - H_{n-1}(z_n), F_{n,1}(z_n) \cdot F_{n,2}(z_n) \cdot \ldots \cdot F_{n,i}(z_n)\}$$

for some appropriate polynomials $H_1, \ldots, H_{n-1} \in \mathbf{Q}[z_n]$. Since $F_{n,1} \cdot F_{n,2} \cdot \ldots \cdot F_{n,i}$ and $F_{n,i+1}$ are relatively prime, as in Step 1, we see that

$$p_1 \cap p_2 \cap \ldots \cap p_i + p_{i+1} = (1).$$

So we have

$$(p_1 \cap p_2 \cap \ldots \cap p_i) \cap p_{i+1} = (p_1 \cap p_2 \cap \ldots \cap p_i) \cdot p_{i+1}.$$

We see that the Gröbner basis of $(p_1 \cap p_2 \cap \ldots \cap p_i) \cap p_{i+1}$ has the form

$$\{z_1 - K_1(z_n), z_2 - K_2(z_n), \ldots, z_{n-1} - K_{n-1}(z_n), F_{n,1} \cdot F_{n,2} \cdot \ldots \cdot F_{n,i+1}\}$$

for suitable polynomials $K_1, K_2, \ldots, K_{n-1}$. Q.E.D.

COROLLARY (Gianni, Trager, Zacharias) (Primary decomposition)
Let $I \subset \mathbf{Q}[x_1, x_2, \ldots, x_n]$ be a zero-dimensional ideal. Under almost all coordinate transformations, if $I \cap \mathbf{Q}[z_n] = (g)$ and g is factored to $g_1^{e_1} \cdot g_2^{e_2} \cdot \ldots \cdot g_s^{e_s}$, then

$$I = (I, g_1^{e_1}) \cap (I, g_2^{e_2}) \cap \ldots \cap (I, g_s^{e_s})$$

is the irredundant primary decomposition of I. □

PROOF. $(\sqrt{I}, g_i)$ is the radical of $(I, g_i^{e_i})$. Q.E.D.

3. Computation of Radicals

Let I be a zero-dimensional ideal of the ring $\mathbf{Q}[x_1, x_2, \ldots, x_n]$, after a suitable coordinate transformation, we have the primary decomposition

$$I = (I, g_1^{e_1}) \cap (I, g_2^{e_2}) \cap \ldots \cap (I, g_s^{e_s}),$$

where $(g) = I \cap \mathbf{Q}[z_n]$ and $g = g_1^{e_1} \cdot g_2^{e_2} \cdot \ldots \cdot g_s^{e_s}$. We denote by q_i the ideal $(I, g_i^{e_i})$ for $i = 1, 2, \ldots, s$.

It is easy to see that $\sqrt{I} = \sqrt{q_1} \cap \sqrt{q_2} \cap \ldots \cap \sqrt{q_s}$, so we have only to compute the radical of each primary ideal.

Hereafter in this section we will write g in place of g_1 and q for $(I, g_1^{e_1})$.

PROPOSITION 3.1. *Let $\{\psi_1, \psi_2, \ldots, \psi_\lambda\}$ be the Gröbner basis of the ideal (q, g), then there exist positive integers l and i such that*

$$(z_{n-1} - \varphi_{n-1}(z_n))^l \equiv \psi_i \mod (g)$$

for some polynomial $\varphi_{n-1}(z_n) \in \mathbf{Q}[z_n]$.

PROOF. Since the Gröbner basis of the $\sqrt{(q, g)}$ $(= \sqrt{q})$ has the form

$$\{z_1 - F_1(z_n), z_2 - F_2(z_n), \ldots, z_{n-1} - F_{n-1}(z_n), F_n(z_n)\},$$

we have a positive integer k such that

$$(z_{n-1} - F_{n-1}(z_n))^k \in q \subset (q, g).$$

Let N be a set of positive integers

$$N = \{\mu \in \mathbf{Z}_+ \mid \exists\, F(z_n) \in \mathbf{Q}[z_n] \text{ such that } (z_{n-1} - F(z_n))^\mu \in (q, g)\}.$$

Since $k \in N$, we see that N is not empty. We let l be the smallest integer in N, and $\psi_{n-1}(z_n)$ be a polynomial satisfying the condition

$$(z_{n-1} - \varphi_{n-1}(z_n))^l \in (q, g).$$

$(z_{n-1} - \varphi_{n-1}(z_n))^l$ may be reduced to $0 \bmod (g)$ by the Gröbner basis $\{\psi_1, \psi_2, \ldots, \psi_\lambda\}$, so there is an element ψ_i and a power product $u = z_{i1}^{\beta_1} \cdot z_2^{\beta_2} \cdot \ldots \cdot z_n^{\beta_n}$, such that

$$z_{n-1}^l = z_1^{\alpha_1} \cdot z_2^{\alpha_2} \cdot \ldots \cdot z_n^{\alpha_n} \times z_1^{\beta_1} \cdot z_2^{\beta_2} \cdot \ldots \cdot z_n^{\beta_n},$$

where $z_1^{\alpha_1} \cdot z_2^{\alpha_2} \cdot \ldots \cdot z_n^{\alpha_n}$ is the leading power product of ψ_i. From this equation, we see that $\alpha_1 = \ldots = \alpha_{n-2} = \alpha_n = 0$, $\beta_1 = \ldots = \beta_{n-2} = \beta_n = 0$, and $0 < \alpha_{n-1} \leqq l$. This shows that the leading power product of ψ_i is $z_{n-1}^{\alpha_{n-1}}$ where $0 < \alpha_{n-1} \leqq l$. Let α be the smallest exponent among the leading power products of elements of the Gröbner basis having the special form z_{n-1}^β. We assume $\mathrm{ht}(\psi_j) = z_{n-1}^\alpha$. (In fact, there is exactly one element with a leading power product of the form z_{n-1}^β, since we are considering a reduced Gröbner basis.) Then ψ_j can be written as

$$\psi_j = z_{n-1}^\alpha + \alpha_1(z_n) \cdot z_{n-1}^{\alpha-1} + \ldots + \alpha_\alpha(z_n),$$

for some polynomials $a_i(z_n) \in \mathbf{Q}[z_n]$.

Regarding $(z_{n-1} - \varphi_{n-1}(z_n))^l$ and φ_j as polynomials in the variable z_{n-1}, we may divide as follows

$$(z_{n-1} - \psi_{n-1}(z_n))^l = (z_{n-1}^{l-\alpha} + b_1(z_n) \cdot z_{n-1}^{l-\alpha-1} + \ldots + b_{l-\alpha}(z_n)) \times \psi_j + c_1(z_n) \cdot z_{n-1}^{\alpha-1} + \ldots + c_\alpha(z_n).$$

Since $(z_{n-1} - \varphi_{n-1}(z_n))^l$ and ψ_j are contained in the ideal (q, g), we see $c_1(z_n) \cdot z_{n-1}^{\alpha-1} + \ldots + c_\alpha(z_n)$ is contained in (q, g).

Suppose that g does not divide $c_1(z_n)$. Since g is irreducible, g and c_1 are relatively prime, so we have two polynomials $B_1(z_n)$ and $B_2(z_n)$ such that

$$B_1 \cdot g + B_2 \cdot c_1 = 1.$$

We have a polynomial

$$B_1 \cdot g \cdot z_{n-1}^{\alpha-1} + B_2 \cdot (c_1 \cdot z_{n-1}^{\alpha-1} + \ldots + c_\alpha) = z_{n-1}^{\alpha-1} + B_2 \cdot c_1 \cdot z_{n-1}^{\alpha-2} + \ldots + B_2 \cdot c_{\alpha-1} \cdot z_{n-1} + B_2 \cdot c_\alpha,$$

which is contained in (q, g). But since α is the smallest exponent of z_{n-1} among $\mathrm{ht}(\psi_i)$ for i such that $\mathrm{ht}(\psi_i)$ has the form z_{n-1}^β, this leads to the contradiction that the polynomial $z_{n-1}^{\alpha-1} + \ldots + B_2 \cdot c_\alpha$ cannot be reduced to 0, so $g | c_1$.

In the same manner, we see $g | c_1, \ldots, g | c_{\alpha-1}$. It is easy to see that $c_\alpha(z_n)$ is contained in $(q, g) \cap \mathbf{Q}[z_n] = (g)$ and $g | c_\alpha$. Hence

$$(z_{n-1} - \varphi_{n-1})^l \equiv (z_{n-1}^{l-\alpha} + b_1(z_n) \cdot z_{n-1}^{l-\alpha-1} + \ldots + b_{l-\alpha}(z_n)) \times k_j \mod (g). \tag{3.1}$$

Here we note that the above equation yields the equation

$$(z_{n-1} - a)^l = (z_{n-1}^{l-\alpha} + b_1 \cdot z_{n-1}^{l-\alpha-1} + \ldots + b_{l-\alpha}) \times \psi_j(z_{n-1})$$

in the ring $\mathbf{Q}(\xi)[z_{n-1}]$, where ξ is an algebraic element whose minimal polynomial is g, $a = \varphi_{n-1}(\xi)$, and $\psi_j(z_{n-1})$ may be regarded as a polynomial in this ring. From this relation, we see that all roots of ψ_j must be a, so $\psi_j(z_{n-1}) = (z_{n-1} - a)^\alpha$. That is

$$\psi_j(z_{n-1}) \equiv (z_{n-1} - \varphi_{n-1}(z_n))^\alpha \mod (g).$$

On the other hand, since $l = \min N$, $l \leqq \alpha$. So we have $\alpha = l$. Q.E.D.

When we compute the Gröbner basis, $\psi_i(z_{n-1})$ appears in an expanded form

$$\psi_i(z_{n-1}) = z_{n-1}^l - \alpha_1(z_n) \cdot z_{n-1}^{l-1} + \ldots + a_l(z_n).$$

The above proof shows that ψ_i is factored as follows

$$\psi_i \equiv (z_{n-1} - a_1(z_n)/l)^l \mod (g).$$

Therefore, we get $\varphi_{n-1}(z_n) = a_1(z_n)/l$.

Proposition 3.2. *Let $\varphi_{n-1}(z_n)$ be the polynomial given in Proposition 3.1. Let $\{\omega_1, \omega_2, \ldots, \omega_\mu\}$ be the Gröbner basis of the ideal $(q, z_{n-1} - \varphi_{n-1}, g)$, then there is an element ω_i in the Gröbner basis such that*

$$(z_{n-2} - \varphi_{n-2}(z_n))^l \equiv \omega_i \mod (g)$$

for some polynomial $\varphi_{n-2}(z_n)$ and some positive integer l. □

Proof. As in the proof of the previous proposition, there exists a polynomial $F(z_n)$ and a positive integer k such that

$$(z_{n-2} - F(z_n))^k \in (q, z_{n-1} - \varphi_{n-1}, g).$$

Let N be the set

$$N = \{\nu \in \mathbf{Z}_+ \mid \exists\, F(z_n) \in \mathbf{Q}[z_n] \text{ such that } (z_{n-2} - F(z_n))^\nu \in (q, z_{n-1} - \varphi_{n-1}, g)\}.$$

N is not empty. We let $l = \min N$, and we suppose that the polynomial $\varphi_{n-2}(z_n)$ satisfies the condition $(z_{n-2} - \varphi_{n-2}(z_n))^l \in (q, z_{n-1} - \varphi_{n-1}, g)$. As in the proof of Proposition 3.1, there exists an element ω_i of the Gröbner basis such that $\mathrm{ht}(\omega_i) = z_{n-22}^\alpha$ with $0 < \alpha \leqq l$. Since the Gröbner basis is reduced, z_{n-2}^α is the smallest power of z_{n-2} which occurs as the head term of any member of the ideal.

ω_i may be written as

$$\omega_i = z_{n-2}^\alpha + a_1(z_{n-1}, z_n) \cdot z_{n-2}^{\alpha-1} + \ldots + a_\alpha(z_{n-1}, z_n),$$

but since we are considering a reduced Gröbner basis, ω_i has already been reduced by $z_{n-1} - \varphi_{n-1}(z_n)$, so ω_i may be written as

$$\omega_i = z_{n-2}^\alpha + a_1(z_n) \cdot z_{n-2}^{\alpha-1} + \ldots + a_\alpha(z_n).$$

As in the proof of the previous proposition, we see

$$(z_{n-2} - \varphi_{n-2}(z_n))^l \equiv (z_{n-2}^{l-\alpha} + b_1(z_n) \cdot z_{n-2}^{l-\alpha-1} + \ldots + b_{l-\alpha}(z_n)) \times \omega_i \mod (g).$$

From this equation, we have that $\omega_i = (z_{n-2} - \varphi_{n-2}(z_n))^\alpha \mod (g)$. As in the previous proposition, $\alpha = l$. Q.E.D.

Likewise we can find in the Gröbner basis of the ideal

$$(q, z_{n-2} - \varphi_{n-2}(z_n), z_{n-1} - \varphi_{n-1}(z_n), g),$$

an element which is equal to $(z_{n-3} - \varphi_{n-3}(z_n))^l$ modulo (g) for some polynomial $\varphi_{n-3}(z_n)$ and some positive integer l. Repeating this process, we find polynomials $\varphi_1(z_n), \varphi_2(z_n), \ldots, \varphi_{n-1}(z_n)$.

It is easy to see that $\{z_1-\varphi_1(z_n), \ldots, z_{n-1}-\varphi_{n-1}(z_n), g\}$ is the Gröbner basis of the radical of q. The algorithm is as follows.

ALGORITHM 3 [Computation of radicals]

```
% input: polynomials {f_1, ..., f_m} in Q[z_1, ..., z_n];
% assumptions: the coordinates have been suitably transformed,;
%              and I = (f_1, ..., f_m) is zero-dimensional.;
% output: Gröbner bases of √p_i's,;
%         where I = p_1 ∩ p_2 ∩ ... ∩ p_s (primary decomposition).;
G := the reduced Gröbner basis of (f_1, ..., f_m);
g(z_n) := the polynomial in G ∩ Q[z_n];
g = g_1^{e_1} · ... · g_s^{e_s};        % factorisation;
for i := 1 to s do
  begin G_i := the reduced Gröbner basis of (G, g_i);
    for j := n-1 down to 1 do
      begin ψ := the polynomial in G_i ∩ Q[z_j, z_n]
            such that z_j^l - a_1(z_n)·z_j^{l-1} + ... + a_l(z_n);
        p := z_j - a_1(z_n)/l;
        G_i := the reduced Gröbner basis of (G_i, p);
    end;
  end;
return G_1, ..., G_s;  □
```

This algorithm is based on the property of a lexicographic order Gröbner basis, whose computational complexity is very large. However, the univariate polynomial g is obtained efficiently using a total degree order Gröbner basis, as is discussed in Kobayashi *et al.* (1988).

4. Concluding Remarks

We have proved that a lexicographic Gröbner basis of zero-dimensional ideal I has the form (1.2) when $\sqrt{I}=I$, and we have presented an algorithm to compute $\sqrt{I}$ from I. Under the condition $\sqrt{I}=I$, a new method for solving a system of algebraic equations can be applied, which is practical for large problems and guarantees numerical accuracy [see Kobayashi *et al.* (1988) for details]. Nevertheless, the choice of transformation of coordinates is still heuristic and trial and error may be necessary to find the generic coordinate system.

We would like to express our sincere gratitude to Dr T. Sasaki, Mr H. Murao, Mr A. Furukawa and Mr T. Fujise for valuable and helpful discussions and assistance. We also would like to express special thanks to Professor B. Buchberger for reading an early manuscript.

References

Buchberger, B. (1970). Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems. *Aequationes Mathematicae* **4/3**, 374–383.

Buchberger, B. (1985). Gröbner bases: an algorithmic method in polynomial ideal theory. In: (Bose, N. K., ed.) *Progress, Directions and Open Problems in Multidimensional Systems Theory*, chap. 6. Dordrecht: D. Reidel.

Gianni, P., Trager, B., Zacharias, C. (1988). Gröbner bases and primary decomposition of polynomial ideals. *J. Symb. Comp.* **6**, 149–168.

Gröbner, W. (1949). *Moderne Algebraische Geometrie*. Berlin: Springer.

Kobayashi, H., Moritsugu, S., Hogan, R. W. (1988). Solving systems of algebraic equations. *Proc. ISSAC '88*, to be published.

Trinks, W. L. (1978). Über Buchbergers Verfahren, Systeme algebraischer Gleichungen zu lösen. *J. Number Theory* **10/4**, 475–488.

Trinks, W. L. (1984). On improving approximate results of Buchberger's algorithm by Newton's method. *SIGSAM Bulletin* **18/3**, 7–11.

van der Waerden, B. L. (1931). *Moderne Algebra*. Berlin: Springer.