J. Symbolic Computation (1992) **14**, 399–417

Solutions of Systems of Algebraic Equations and Linear Maps on Residue Class Rings

KAZUHIRO YOKOYAMA, MASAYUKI NORO AND TAKU TAKESHIMA

International Institute for Advanced Study of Social Information Science
FUJITSU LABORATORIES LTD., 140 Miyamoto, Numazu-shi, 410-03, JAPAN

(*Received* 8 *June* 1990)

In this paper, we present new mathematical results and several new algorithms for solving a system of algebraic equations algebraically. We find that many ideal-theoretical arguments for the problem can be translated into their counterparts in the theory of linear maps. And by this translation, we succeed in giving a new description for the U-resultant and forms of solutions of systems straightforwardly. New algorithms proposed here apply algorithms of linear algebra to avoid repeated computations of Gröbner bases under lexicographic order, and they require computation of a Gröbner basis, under arbitrary order, only once in principle. The new algorithms improve the efficiency of computation.

1. Introduction

For solving a simultaneous system of algebraic equations, the method using general elimination is well-known and an algorithm of calculation of the U-resultant was introduced in van der Waerden (1936). But it was almost impossible to execute the calculation actually before Lazard (1981) presented an algorithm based on general elimination. But actually, it also could not solve *large* systems and systems with non-rational solutions. Meanwhile, as another method, Buchberger (1970) and Trinks (1978) showed a method using a Gröbner basis for the ideal generated by a system. Still, it seemed difficult to calculate the solutions for *large* systems by their method, since it needed the computation of Gröbner basis under the lexicographic order and computations in algebraic extension fields. Compared with methods using general elimination, methods using Gröbner basis have the advantage that the solutions are obtained as roots of univariate polynomials. On the other hand, methods using general elimination can express the multiplicity of the solutions explicitly via the U-resultant. But as pointed out in Lazard (1983), the above two methods have the same mathematical basis and so they are very similar.

Recently, the two were improved. In Kobayashi *et al.* (1988), a new algorithm based on Lazard's idea is presented and it uses Gröbner bases under the total degree order for the calculation of the U-resultant and factorization of univariate polynomials for the calculation of the solutions. In Kobayashi *et al.* (1988, 1989), new algorithms which compute the solution as an n-tuple of univariate polynomials in the roots of a certain univariate polynomial are presented. This polynomial representation of solutions follows

0747-7171/92/100399+19 $08.00/0

from a Gröbner basis in a *special form*. These algorithms are composed by combining a primary decomposition algorithm in Gianni *et al.* (1988) and an algorithm for solving linear equations, by which they succeed in replacing computation of Gröbner bases under the lexicographic order with that under the total degree order. Also in Lazard (1992), a very similar algorithm is presented by introducing a new concept *triangular set*, which is more general than one of Gröbner basis in a special form. But, it needs an additional procedure to express the solutions in the same form as in Kobayashi *et al.*'s algorithms.

In this paper, we give a new presentation of the theory of the solution sets of systems of algebraic equations in relation to Gröbner bases in view of the theory of linear maps, by which we can reconstruct and unify the theory in Lazard (1981) and that in Kobayashi *et al.* (1988). More precisely, for a system of algebraic equations in n variables $x_1, ..., x_n$ we consider the residue class ring factored by the ideal generated by the system, and we find that the linear maps X_i on the residue class ring which multiply each element by x_i can be represented simultaneously as upper-triangular matrices with respect to some suitable base (Lemma 2.2). By using this representation, we can provide a simple and well understandable presentation of the U-resultant in the affine case (Theorem 2.4, Theorem 2.5) and show several related known theorems straightforwardly (Section 3). Moreover, we show additional results on the solutions of systems and associated ideals, and new algorithms, based on that theory, for solving a system of algebraic equations, which are believed to improve algorithms in Kobayashi *et al.* (1988, 1989).

In Section 2 we give a new presentation of the theory of the solution sets of systems of algebraic equations, and reconstruct the theory in Lazard (1981) and in Kobayashi *et al.* (1988) by the new presentation. Then, in Section 3 we clarify several known theorems related to 0-dimensional ideals and also give a further detailed study on the solution of a system of algebraic equations by using the theory in Section 2. In Section 4 we show several new algorithms for solving a system using the result in Section 3.

2. A New Presentation of the Theory of Solutions of Systems

Let $\mathcal{S} = \{f_1(x_1, ..., x_n) = 0, ..., f_k(x_1, ..., x_n) = 0\}$ be a system of algebraic equations in n variables $x_1, ..., x_n$ over the field $\mathbb{Q}$ of rational numbers with finitely many solutions. Let $\mathcal{P}$ be the ring of polynomials $\mathbb{Q}[x_1, ..., x_n]$. We denote by $\mathcal{I}$ the ideal $(f_1, ..., f_k)$ generated by $f_1, ..., f_k$ in $\mathcal{P}$, and also denote by $\mathcal{A}$ the residue class ring $\mathcal{P}/\mathcal{I}$. Let $p_{\mathcal{A}}$ be the canonical homomorphism from $\mathcal{P}$ to $\mathcal{A}$.

2.1. DEFINITION OF CERTAIN LINEAR MAPS ON RESIDUE CLASS RINGS

Since the number of the solutions of $\mathcal{S}$ is finite, the ideal $\mathcal{I}$ is 0-dimensional and the ring $\mathcal{A}$ is a finite dimensional $\mathbb{Q}$-vector space. We denote by ℓ the dimension of $\mathcal{A}$ as a $\mathbb{Q}$-vector space. Then, it is known that the number of the solutions of $\mathcal{S}$ with multiplicities counted is equal to ℓ.

Moreover, since all solutions of $\mathcal{S}$ are contained in $\mathbb{C}^n$, we have to deal with $\mathbb{C}[x_1, ..., x_n]$ and the ideal $\mathcal{I}_{\mathbb{C}}$ generated by $f_1, ..., f_k$ in $\mathbb{C}[x_1, ..., x_n]$. Then $\mathbb{C}[x_1, ..., x_n] = \mathbb{C} \otimes_{\mathbb{Q}} \mathcal{P}$, which we denote by $\mathcal{P}_{\mathbb{C}}$, and $\mathcal{I}_{\mathbb{C}} = \mathbb{C} \otimes_{\mathbb{Q}} \mathcal{I}$. Consider the residue class ring $\mathcal{P}_{\mathbb{C}}/\mathcal{I}_{\mathbb{C}}$, which we denote by $\mathcal{A}_{\mathbb{C}}$. Then, $\mathcal{A}_{\mathbb{C}} = \mathbb{C} \otimes_{\mathbb{Q}} \mathcal{A}$ and a basis for $\mathcal{A}$ is also a basis for $\mathcal{A}_{\mathbb{C}}$. We denote the canonical homomorphism from $\mathcal{P}_{\mathbb{C}}$ to $\mathcal{A}_{\mathbb{C}}$ by $p_{\mathcal{A}_{\mathbb{C}}}$. We also denote the set of all endomorphisms on $\mathcal{A}$ by $END(\mathcal{A})$, and that on $\mathcal{A}_{\mathbb{C}}$ by $END(\mathcal{A}_{\mathbb{C}})$. Then $END(\mathcal{A})$ becomes a $\mathbb{Q}$-algebra and $END(\mathcal{A}_{\mathbb{C}})$ becomes a $\mathbb{C}$-algebra.

Now we define certain linear maps, which play an important role in the theory of the solutions of systems of algebraic equations, and hence appeared in several papers; Lazard (1981, 1983, 1992), Kobayashi *et al.* (1988) and Auzinger & Stetter (1989).

DEFINITION 2.1. Since $\mathcal{A}$ is a commutative ring, for an element u in $\mathcal{A}$ the map U multiplying each element in $\mathcal{A}$ by u is a linear map on $\mathcal{A}$. Especially, we define a linear map X_i as the linear map multiplying each element in $\mathcal{A}$ by x_i for each i, i.e.,

$$X_i : p_{\mathcal{A}}(u) \in \mathcal{A} \to p_{\mathcal{A}}(u \cdot x_i) = p_{\mathcal{A}}(u) \cdot p_{\mathcal{A}}(x_i) \in \mathcal{A},$$

where $u \in \mathbb{Q}[x_1, ..., x_n]$. Similarly, we extend each linear map X_i to a linear map on $\mathcal{A}_{\mathbb{C}}$, which we denote by the same symbol. Moreover, since these X_i's commute, we define polynomials of the linear maps X_i's as follows.

For a polynomial $h(x_1, ..., x_n) = \sum h_{e_1,...,e_n} x_1^{e_1} \cdots x_n^{e_n}$ in $\mathcal{P}$, we define the linear map $h(X_1, ..., X_n)$ as

$$h(X_1, ..., X_n) = \sum_{(e_1,...,e_n) \neq (0,...,0)} h_{e_1,...,e_n} X_1^{e_1} \cdots X_n^{e_n} + h_{0,...,0} I,$$

where I is the identical map.

Then, we have the following lemma.

LEMMA 2.1. *For a polynomial $h(x_1, ..., x_n)$ in $\mathcal{P}$ (or $\mathcal{P}_{\mathbb{C}}$), $h(x_1, ..., x_n)$ belongs to the ideal $\mathcal{I}$ (or $\mathcal{I}_{\mathbb{C}}$) if and only if the linear map $h(X_1, ..., X_n)$ vanishes on $\mathcal{A}$ (or $\mathcal{A}_{\mathbb{C}}$). Thus, the kernel of the homomorphism from $\mathcal{P}$ into $END(\mathcal{A})$ (or from $\mathcal{P}_{\mathbb{C}}$ into $END(\mathcal{A}_{\mathbb{C}})$) is the ideal $\mathcal{I}$ (or $\mathcal{I}_{\mathbb{C}}$).*

From Lemma 2.1, we may conclude that the natural homomorphism from $\mathcal{A}_{\mathbb{C}}$ into $END(\mathcal{A}_{\mathbb{C}})$ is injective.

Let $\mathcal{G}$ be a fixed Gröbner basis of $\mathcal{I}$ with respect to an arbitrary order. Then Buchberger showed the following. (See Buchberger, 1988.)

BUCHBERGER'S THEOREM. *The set $B_{\mathcal{G}} = \{u |$ u is a power product and u is not divisible by the leading power product of any element of $\mathcal{G}$ $\}$ is a linearly independent basis for $\mathcal{A}$.*

By taking the above set $B_{\mathcal{G}}$ as a basis of $\mathcal{A}$, each linear map X_i is expressed as

$$X_i : NormalForm(u) \in \mathcal{A} \to NormalForm(u \cdot x_i) \in \mathcal{A},$$

where $NormalForm(u)$ is the normal form of u with respect to $\mathcal{G}$. And with respect to the basis $B_{\mathcal{G}}$ we can construct the matrix representation $M_{B_{\mathcal{G}}}(X_i)$ of X_i for $i = 1, ..., n$.

2.2. SOLUTION SETS OF SYSTEMS AND LINEAR MAPS X_i

We present our main observation about the linear maps X_i and the relation between them and the solutions of the system $\mathcal{S}$. Let $\mathcal{X}$ be the subalgebra of $END(\mathcal{A}_{\mathbb{C}})$ generated by $I, X_1, ..., X_n$, where I is the identical map. Since $X_i X_j = X_j X_i$ for $i, j = 1, ..., n$, $\mathcal{X}$ is commutative and so we have a fundamental theorem of linear algebra:

LEMMA 2.2. *There is a basis B for $\mathcal{A}_{\mathbb{C}}$ such that the matrix representations of $X_1, \ldots, X_n$ with respect to B are upper-triangular.*

We provide a brief proof. (See Section 12 and 13 in van der Waerden, 1991.) By Jordan-Hölder's theorem, there is the following sequence of sub $\mathcal{X}$-modules.

$$\mathcal{A}_{\mathbb{C}} = \mathcal{E}_0 \supset \mathcal{E}_1 \supset \cdots \supset \mathcal{E}_t = \{0\},$$

where each $\mathcal{E}_i/\mathcal{E}_{i+1}$ is an irreducible $\mathcal{X}$-module. Since $\mathcal{X}$ is commutative and $\mathbb{C}$ is algebraically closed, Schur's lemma says that the rank of each irreducible $\mathcal{X}$-module $\mathcal{E}_i/\mathcal{E}_{i+1}$ is 1. This implies that by taking one element b_{i+1} from $\mathcal{E}_i \setminus \mathcal{E}_{i+1}$, we obtain a basis $B = \{b_1, \ldots, b_t\}$ for $\mathcal{A}_{\mathbb{C}}$ such that with respect to this basis, every element in $\mathcal{X}$ can be written as an upper-triangular matrix.

We fix the above basis B and denote the matrix representation of each element Y in $\mathcal{X}$ with respect to B by $\mathrm{M}_B(Y)$. By Lemma 2.2, each $\mathrm{M}_B(X_i)$ is written as follows:

$$\mathrm{M}_B(X_i) = \begin{pmatrix} \alpha_{i,1} & * & \cdots & * \\ 0 & \alpha_{i,2} & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \alpha_{i,\ell} \end{pmatrix},$$

where $\ell = \dim_{\mathbb{C}} \mathcal{A}_{\mathbb{C}} =$ the number of the solutions of $\mathcal{S}$. From this, we conclude that for every polynomial $h(x_1, \ldots, x_n)$, the matrix representation $\mathrm{M}_B(h(X_1, \ldots, X_n))$ is upper triangular with diagonal components $h(\alpha_{1,j}, \ldots, \alpha_{n,j})$.

We shall show that the solutions of $\mathcal{S}$ can be constructed from these $\alpha_{i,j}$. We need,

LEMMA 2.3. *Let h be a polynomial in $\mathcal{P}$ and $\mathcal{J}$ be an ideal in $\mathcal{P}$ which is generated by $\mathcal{I}$ and h. Similarly, let $\tilde{h}$ be a polynomial in $\mathcal{P}_{\mathbb{C}}$ and $\tilde{\mathcal{J}}$ be an ideal in $\mathcal{P}_{\mathbb{C}}$ which is generated by $\mathcal{I}_{\mathbb{C}}$ and $\tilde{h}$. Then,*

$$\mathbb{Q}[x_1, \ldots, x_n]/\mathcal{J} = \mathcal{A}/h(X_1, \ldots, X_n)\mathcal{A},$$
$$\mathbb{C}[x_1, \ldots, x_n]/\tilde{\mathcal{J}} = \mathcal{A}_{\mathbb{C}}/\tilde{h}(X_1, \ldots, X_n)\mathcal{A}_{\mathbb{C}}.$$

Now we show the following which gives an alternative proof of the mathematical basis for constructions of the U-resultant in Kobayashi *et al.* (1988). First we give an elementary proof based on the theory of linear algebra.

THEOREM 2.4. *Let $\alpha_j = (\alpha_{1,j}, \ldots, \alpha_{n,j})$. Then, the set consisting of all distinct α_j coincides with the set of all distinct solutions of the system $\mathcal{S}$.*

PROOF. Let $\beta_1 = (\beta_{1,1}, \ldots, \beta_{n,1}), \ldots, \beta_{\ell'} = (\beta_{1,\ell'}, \ldots, \beta_{n,\ell'})$ be all distinct solutions of the system $\mathcal{S}$. First we show that every α_j is a solution of the system $\mathcal{S}$. For each α_j, we set $U_j = \{u = (u_0, u_1, \ldots, u_n) \text{ in } \mathbb{C}^{n+1} \mid u_0 + \alpha_{1,j} \cdot u_1 + \cdots + \alpha_{n,j} \cdot u_n = 0\}$, and for each β_k, we also set $V_k = \{v = (v_0, v_1, \ldots, v_n) \text{ in } \mathbb{C}^{n+1} \mid v_0 + \beta_{1,k} \cdot v_1 + \cdots + \beta_{n,k} \cdot v_n = 0\}$. U_j is the orthocomplement of $(1, \alpha_{1,j}, \ldots, \alpha_{n,j})$ and V_k is the orthocomplement of $(1, \beta_{1,k}, \ldots, \beta_{n,k})$.

For each element $u = (u_0, u_1, \ldots, u_n)$ in U_j, the linear map $u(X) = u_0 I + u_1 X_1 + \cdots + u_n X_n$ degenerates, i.e., $\mathrm{Ker}(u_0 I + u_1 X_1 + \cdots + u_n X_n) \neq \{0\}$, since the matrix $\mathrm{M}_B(u(X))$ is upper triangular and its (j,j)-component is $u_0 + \alpha_{1,j} \cdot u_1 + \cdots + \alpha_{n,j} \cdot u_n = 0$. Therefore we have $\mathcal{A}_{\mathbb{C}}/u(X)\mathcal{A}_{\mathbb{C}} \neq \{0\}$. By Lemma 2.3, this implies that $\mathbb{C}[x_1, \ldots, x_n]/(\mathcal{I}, u_0 + u_1 x_1 +$

$\cdots + u_n x_n) \neq \{0\}$, and $\mathcal{I}$ and $u_0 + u_1 x_1 + \cdots + u_n x_n$ have a common zero. From this, u belongs to some V_k. Thus, U_j is included in $\cup_{k=1}^{\ell'} V_k$, i.e., $U_j = \cup_{k=1}^{\ell'}(U_j \cap V_k)$. Since U_j, V_k are hyper-planes, U_j coincides with some V_k. Hence, α_j is a solution of the system $\mathcal{S}$.

Next we show that every solution β_i is contained in the set $\{\alpha_j | j = 1, ..., \ell\}$. Assume, to the contrary, that some β_i is not contained in the set $\{\alpha_j | j = 1, ..., \ell\}$. Then there is a polynomial $h(x_1, ..., x_n)$ in $\mathcal{A}_C$ which has β_i as a zero, but has not any α_j as a zero. The linear map $h(X_1, ..., X_n)$ is non-degenerate on $\mathcal{A}_C$ since the upper triangular matrix $\mathrm{M}_B(h(X_1, ..., X_n))$ has non zero diagonal components $h(\alpha_{1,j}, ..., \alpha_{n,j})$. Therefore we have $h(X_1, ..., X_n)\mathcal{A}_C = \mathcal{A}_C$ and so $\mathcal{A}_C/h(X_1, ..., X_n)\mathcal{A}_C = \{0\}$. By Lemma 2.3, the ideal $(\mathcal{I}_C, h)$ coincides with $\mathbb{C}[x_1, ..., x_n]$. So $(\mathcal{I}_C, h)$ has no zeros. But β_i is a common zero of $\mathcal{I}_C$ and h. This is a contradiction. □

From now on, we shall denote the family $\{\alpha_j | j = 1, ..., \ell\}$ by $\mathcal{V}$. Then, $\mathcal{V}$ coincides with the set of all solutions of the system $\mathcal{S}$ with multiplicities counted. Now we give a brief proof for this fact, which also shows Theorem 2.4 directly. (In Yokoyama *et al.*, 1989a and 1990, we gave an elementary proof.)

The multiplicity of a solution $\alpha_j = (\alpha_{1,j}, ..., \alpha_{n,j})$ is the multiplicity of the maximal ideal $\mathcal{M}_j = (x_1 - \alpha_{1,j}, ..., x_n - \alpha_{n,j})$ in the ring $\mathcal{A}_C$ which is Artinian. According to the definition of multiplicity, the multiplicity of $\mathcal{M}_j$ is the length of the localization of $\mathcal{A}_C$ at $\mathcal{M}_j$. (See Hartshorne, 1977, or Zariski & Samuel, 1960.) Moreover, since $\mathcal{A}_C$ is decomposed into the sequence of modules $\mathcal{E}_0/\mathcal{E}_1, \mathcal{E}_1/\mathcal{E}_2, ..., \mathcal{E}_{\ell-1}/\mathcal{E}_\ell$, the length of the localization of $\mathcal{A}_C$ at $\mathcal{M}_j$ is the number of all $\mathcal{E}_k/\mathcal{E}_{k+1}$ which are isomorphic to $\mathcal{P}_C/\mathcal{M}_j$, that is, on which $\mathcal{M}_j$ annihilates. It is easily proven that $\mathcal{M}_j$ annihilates on $\mathcal{E}_k/\mathcal{E}_{k+1}$ if and only if the k-th diagonal component of each X_i coincides with $\alpha_{i,j}$. This implies that the set $\mathcal{V}$ coincides with the set of all solutions of $\mathcal{S}$ with multiplicities counted.

THEOREM 2.5. *$\mathcal{V}$ coincides with the set of all solutions of $\mathcal{S}$ with multiplicities counted.*

By Theorem 2.5, the determinant of the matrix $U_0 I + U_1 \mathrm{M}_B(X_1) + \cdots + U_n \mathrm{M}_B(X_n)$ gives the U-resultant of $\mathcal{S}$, where $U_0, ..., U_n$ are indeterminates. And $U_0 I + U_1 \mathrm{M}_{B_\sigma}(X_1) + \cdots + U_n \mathrm{M}_{B_\sigma}(X_n)$ also gives the same. This is Kobayashi *et al.*'s presentation of the U-resultant.

From the proof of Theorem 2.4 and the matrix representation, we have

COROLLARY 2.6. *Let h be a polynomial in $\mathbb{C}[x_1, ..., x_n]$. Then, the following are equivalent;*

(1) *the linear map $h(X_1, ..., X_n)$ degenerates,*

(2) *$\mathcal{I}_C$ and h have a common zero.*

Moreover, if $\mathcal{I}_C$ has no multiple zeros, the number of the common zeros of $\mathcal{I}_C$ and h is equal to the dimension of the kernel of $h(X_1, ..., X_n)$.

REMARK 2.1. Each eigenvalue of the linear map X_i is the x_i-component of some solution of the system. This fact is already known and was proved first by Lazard (1981). And the problem is how to construct the solutions from these eigenvalues correctly. Many efforts were made for it. Lazard (1981) and Kobayashi *et al.* (1988) have used indeterminates, i.e., the U-resultant, for solving the problem. Lazard (1981) also has dealt with methods

binding eigenvalues of two linear maps X_i and X_j for the x_i-component and the x_j-component of same solution. Auzinger & Stetter (1989) have shown a method for solving systems numerically, which is very similar to one in Lazard (1981). In their paper, they also observed the relation between the eigenvalues of the linear maps and the solutions of the system, and, to construct the solutions, they used the eigenvectors. Their approach is also applicable in our description. (See Remark 2.2.)

Finally in this section, we discuss a detailed structure of the matrix representation of $\mathcal{X}$. By the theory of Jordan's normal forms of matrices, we have the following.

The residue class ring $\mathcal{A}_C$ is decomposed to its non-zero $\mathcal{X}$-invariant subspaces $W_1,\ldots,W_{\ell'}$ such that $W_j = \{y \in \mathcal{A}_C | (X_1 - \beta_{1,j}I)^{e_1}y = 0, (X_2 - \beta_{2,j}I)^{e_2}y = 0, \ldots, (X_n - \beta_{n,j}I)^{e_n}y = 0$ *for some* $e_1,\ldots,e_n\}$ where each $\beta_{i,j}$ is an eigenvalue of X_i for $i = 1,\ldots,n$. Moreover, for each W_j, $(\beta_{1,j},\ldots,\beta_{n,j})$ is a zero of the ideal $\mathcal{I}$ and the dimension of W_j as a linear space coincides with the multiplicity E_j of $(\beta_{1,j},\ldots,\beta_{n,j})$ as a zero of $\mathcal{I}$. Then, we have the following.

LEMMA 2.7. *For some basis* $B' = \{b'_{1,1},\ldots,b'_{1,E_1},b'_{2,1},\ldots,b'_{2,E_2},\ldots,b'_{\ell',E_{\ell'}}\}$, *where* $B'_j = \{b'_{j,1},\ldots,b'_{j,E_j}\}$ *is a basis for* W_j, *each linear map* X_i *is presented as follows:*

$$\mathrm{M}_{B'}(X_i) = \begin{pmatrix} \beta_{i,1}\mathrm{I}_1 + \mathrm{N}_{i,1} & 0 & \cdots & 0 \\ 0 & \beta_{i,2}\mathrm{I}_2 + \mathrm{N}_{i,2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \beta_{i,\ell'}\mathrm{I}_{\ell'} + \mathrm{N}_{i,\ell'} \end{pmatrix},$$

where I_j *is the identity matrix and* $\mathrm{N}_{i,j}$ *is an upper triangular nilpotent matrix.*

REMARK 2.2. For each solution $(\beta_{1,j},\ldots,\beta_{n,j})$ there is a common eigenvector y_j such that $X_iy_j = \beta_{i,j}y_j$ for $i = 1,\ldots,n$. Therefore, if some linear map X_k has no multiple eigenvalue, then each subspace W_j has the dimension 1. From this, for each eigenvalue $\beta_{k,j}$ of X_k its eigenvector y_j is a common eigenvector of $X_1,\ldots,X_n$, i.e., $X_iy_j = \beta_{i,j}y_j$, where $(\beta_{1,j},\ldots,\beta_{n,j})$ is a solution. Thus, under an appropriate condition, we can use eigenvectors for constructing the solutions. This approach was proposed in Auzinger & Stetter (1989).

3. Theoretical Results on the Ideal $\mathcal{I}$ from Section 2

First we show that several known results can be proved straightforwardly from our presentation; next we study them further.

3.1. THE RADICAL OF THE IDEAL $\mathcal{I}$ AND THE PRIMARY DECOMPOSITION

For each i, let the characteristic polynomial of X_i be $H_{X_i}(t)$, and the minimal polynomial of X_i be $M_{X_i}(t)$, where t is a new variable. Since $M_{X_i}(X_i)$ vanishes on $\mathcal{A}_C$, $M_{X_i}(x_i)$ belongs to $\mathcal{I}_C$, and so $H_{X_i}(x_i)$ belongs to $\mathcal{I}_C$ by Lemma 2.3. Moreover, since $\mathrm{M}_{B_G}(X_i)$ has rational entries, $M_{X_i}(t)$ and $H_{X_i}(t)$ have rational coefficients and so $M_{X_i}(x_i)$ and $H_{X_i}(x_i)$ belong to $\mathcal{I}$. By the definition of the minimal polynomial and Lemma 2.3, $M_{X_i}(x_i)$ has minimal degree among all univariate polynomials in x_i belonging to $\mathcal{I}$.

Let $h_i(t)$ be the *square free part* of $H_{X_i}(t)$, i.e.,

$$h_i(t) = H_{X_i}(t)/\mathrm{GCD}(H_{X_i}(t), H'_{X_i}(t)),$$

where $H'_{X_i}(t)$ is the derivative of $H_{X_i}(t)$. Then, h_i is also the square free part of M_{X_i}.

By Lemma 2.7 and the theory of linear algebra, we have the following.

LEMMA 3.1. *If the minimal polynomial M_{X_i} is square free, then the matrix representation $M_{B'}(X_i)$ is diagonal for a suitable basis B'.*

We can show the following theorem which corresponds to Lemma 92 in Seidenberg (1974) and Section 9 in Gianni *et al.* (1988).

THEOREM 3.2. *The ideal $(\mathcal{I}, h_1(x_1), ..., h_n(x_n))$ is the radical $\sqrt{\mathcal{I}}$ of $\mathcal{I}$, and the ideal $(\mathcal{I}_C, h_1(x_1), ..., h_n(x_n))$ is also the radical $\sqrt{\mathcal{I}_C}$ of $\mathcal{I}_C$. Thus, the ideal $\mathcal{I}$ coincides with its radical if and only if every minimal polynomial M_{X_i} is square free.*

PROOF. Let $\mathcal{J} = (\mathcal{I}, h_1(x_1), ..., h_n(x_n))$. Then, by the definition of radicals, $\sqrt{\mathcal{I}} \supset \mathcal{J} \supset \mathcal{I}$. Therefore, it suffices to show that $\mathcal{J}$ coincides with its radical. Since the linear maps X_i on $\mathcal{P}/\mathcal{J}$ are considered as the restrictions of X_i on $\mathcal{A}$ to $\mathcal{P}/\mathcal{J}$, it is clear that the minimal polynomial of X_i on $\mathcal{P}/\mathcal{J}$ coincides with h_i. From this, we may assume that $\mathcal{I}$ contains all h_i and we will show that $\mathcal{I}$ coincides with its radical.

Consider a polynomial $a(x_1, ..., x_n)$ in $\sqrt{\mathcal{I}}$. Then, $a(x_1, ..., x_n)^m$ belongs to $\mathcal{I}$ for some integer m. We take a basis B' as in Lemma 3.1 for which the matrix representation $\mathrm{M}_{B'}(X_i)$ is diagonal. As $\mathcal{X}$ is commutative, the matrix representation $\mathrm{M}_{B'}(a(X_1, ..., X_n))$ is also diagonal with diagonal components $a(\beta_{1,j}, ..., \beta_{n,j})$. From this, the fact that $a(X_1, ..., X_n)^m = 0$ in $END(\mathcal{A})$ implies that each diagonal component $a(\beta_{1,j}, ..., \beta_{n,j})^m$ coincides with 0, and so $a(\beta_{1,j}, ..., \beta_{n,j}) = 0$. Thus, $\mathrm{M}_B(a(X_1, ..., X_n)) = 0$ in $END(\mathcal{A})$ and $a(x_1, ..., x_n)$ belongs to $\mathcal{I}$. Hence, $(\mathcal{I}, h_1, ..., h_n)$ is the radical of $\mathcal{I}$. By the same argument, $(\mathcal{I}_C, h_1, ..., h_n)$ is the radical of $\mathcal{I}_C$. □

Now we consider other linear maps which are expressed as linear sums of the X_i. Let $\mathbb{Z}$ be the set of all integers, and let $\mathbb{Z}^n$ be the direct product of $\mathbb{Z}$ with itself n times. For each element $a = (a_1, ..., a_n)$ in $\mathbb{Z}^n$, we define a linear map $a(X)$ on $\mathcal{A}_C$ as follows:

$$a(X) = a_1X_1 + \cdots + a_nX_n.$$

Similarly we define an algebraic number $a(\alpha_k)$ as follows:

$$a(\alpha_k) = a_1\alpha_{1,k} + \cdots + a_n\alpha_{n,k}.$$

DEFINITION 3.1. For an element $a = (a_1, ..., a_n)$ in $\mathbb{Z}^n$, we call a a *sufficient* vector if a satisfies the following conditions:

(a) $a(\alpha_k)$ is a primitive element of the algebraic extension field of $\mathbb{Q}$ generated by $\alpha_{1,k}, ..., \alpha_{n,k}$ for $1 \leq k \leq \ell$, and
(b) $a(\alpha_k) \neq a(\alpha_j)$ if $\alpha_k \neq \alpha_j$ for $1 \leq j, k \leq \ell$.

By Yokoyama *et al.* (1989b), condition (b) includes condition (a), and *almost every*

element a in $\mathbb{Z}^n$ is a sufficient vector. In section 4.2, we will give a further discussion on the choice of such an element.

Now fix a sufficient vector a in $\mathbb{Z}^n$. We denote the linear map $a(X)$ by Y. Then, with respect to a suitable basis B, $\mathrm{M}_B(Y)$ is upper triangular with diagonal components $a(\alpha_i)$. We consider the characteristic polynomial $H_Y(t)$ and the minimal polynomial $M_Y(t)$ of Y. Since Y is a $\mathbb{Q}$-linear sum of the X_i, $H_Y(t)$ and $M_Y(t)$ are polynomials over $\mathbb{Q}$.

Suppose that H_Y is factorized into its irreducible factors over $\mathbb{Q}$ as follows:

$$H_Y = (H_{Y,1})^{e_1} \cdots (H_{Y,s})^{e_s}.$$

Then, M_Y is factorized into its irreducible factors over $\mathbb{Q}$ as follows:

$$M_Y = (H_{Y,1})^{e'_1} \cdots (H_{Y,s})^{e'_s},$$

where $1 \leq e'_j \leq e_j$. Let h_Y be the square free part of H_Y, i.e.,

$$h_Y = H_{Y,1} \cdots H_{Y,s}.$$

Let $\mathcal{V}_j$ be the set of all solutions α_k such that $(H_{Y,j}(a(\alpha_k))) = 0$. For each α_k in $\mathcal{V}_j$, there are exactly e_j elements equal to α_k in $\mathcal{V}$.

LEMMA 3.3. *For each $\mathcal{V}_j$, there are univariate polynomials $\beta_{1,j}(y), ..., \beta_{n,j}(y)$ uniquely determined over $\mathbb{Q}$ such that*

(1) $\alpha_{i,k} = \beta_{i,j}(a(\alpha_k))$ *for* $\alpha_k \in \mathcal{V}_j$,

(2) degree $\beta_{i,j} <$ degree $H_{Y,j}$.

PROOF. Let α_k be an element of $\mathcal{V}_j$. Since $a(\alpha_k)$ is a primitive element of $\mathbb{Q}(\alpha_{1,k}, ..., \alpha_{n,k})$, each $\alpha_{i,k}$ can be expressed as a $\mathbb{Q}$-polynomial β'_i in $a(\alpha_k)$, and β'_i is uniquely determined modulo $h_{Y,j}$. Let $\sigma_1, ..., \sigma_w$ be all the distinct embeddings of $\mathbb{Q}(\alpha_{1,k}, ..., \alpha_{n,k})$ into $\mathbb{C}$. Then, the number w coincides with the degree of $H_{Y,j}$, and the images $\sigma_1(a(\alpha_k)),..., \sigma_w(a(\alpha_k))$ are all the distinct roots of $H_{Y,j}$. Since α_k is a solution of the system $\mathcal{S}$, each $\sigma_t(\alpha_k)$ is also its solution. As $a(\sigma_t(\alpha_k)) = \sigma_t(a(\alpha_k))$, each $\sigma_t(\alpha_k)$ belongs to $\mathcal{V}_j$. Then, for each σ_t there is an element α_m in $\mathcal{V}_j$ such that

$$\alpha_{i,m} = \sigma_t(\alpha_{i,k}) = \sigma_t(\beta'_i(a(\alpha_k))) = \beta'_i(\sigma_t(a(\alpha_k))) = \beta'_i(a(\sigma_t(\alpha_k))) = \beta'_i(a(\alpha_m)).$$

Thus, for the distinct w elements in $\mathcal{V}_j$ their x_i-th components can be expressed by the polynomial β'_i in them. By letting $\beta_{i,j} = \beta'_i$, we have (1) and (2). The uniqueness of $\beta_{i,j}$ follows from the uniqueness of β'_i. □

By the Chinese remainder theorem, since all $H_{Y,j}$ are mutually relatively prime, there are univariate polynomials $\beta_1(y), ..., \beta_n(y)$ uniquely determined over $\mathbb{Q}$ such that

(1) $\beta_i(y) \equiv \beta_{i,j}(y) \bmod H_{Y,j}$ for $1 \leq j \leq s$ and $1 \leq i \leq n$, and

(2) degree $\beta_i <$ degree h_Y =degree $H_{Y,1} + \cdots +$ degree $H_{Y,s}$.

THEOREM 3.4. *There are integers m_i such that the ideal $\mathcal{I}$ contains $(x_i - \beta_i(a_1x_1 + \cdots + a_nx_n))^{m_i}$ for $i = 1, ..., n$.*

PROOF. Consider the linear map $X_i - \beta_i(Y)$. Its matrix representation $\mathrm{M}_B(X_i - \beta_i(Y))$

is upper triangular with diagonal components $\alpha_{i,j} - \beta_i(a(\alpha_j))$. For each α_k in $\mathcal{V}_j$, since each element in $\mathcal{V}_j$ gives a zero of $H_{Y,j}$, we have $\beta_i(a(\alpha_k)) = \beta_{i,j}(a(\alpha_k))$. By Lemma 3.3, we have $\beta_i(a(\alpha_k)) = \alpha_{i,k}$. From this, $\mathrm{M}_B(X_i - \beta_i(Y))$ is upper triangular with diagonals 0 and so it is nilpotent. Therefore, there exists a positive integer m_i such that $(X_i - \beta_i(Y))^{m_i} = 0$. By Lemma 2.3, $(x_i - \beta_i(a_1x_1 + \cdots + a_nx_n))^{m_i}$ belongs to $\mathcal{I}$. □

For the radical of $\mathcal{I}$, we have the following, which corresponds to Proposition 2.2 in Kobayashi *et al.* (1989), directly from Theorem 3.4.

COROLLARY 3.5. *The radical $\sqrt{\mathcal{I}}$ of $\mathcal{I}$ contains $x_i - \beta_i(a_1x_1 + \cdots + a_nx_n)$ for $i = 1, \ldots, n$.*

Now we consider the decomposition of the ideal $\mathcal{I}$. Let $\mathcal{J}_j$ be the ideal $(H_{Y,j}(a_1x_1 + \cdots + a_nx_n), x_1 - \beta_{1,j}(a_1x_1 + \cdots + a_nx_n), \ldots, x_n - \beta_{n,j}(a_1x_1 + \cdots + a_nx_n))$. Then, it follows that

$$\mathcal{P}/\mathcal{J}_j \cong \mathbb{Q}(\alpha_{1,k}, \ldots, \alpha_{n,k}) \text{ for each } \alpha_k \text{ in } \mathcal{V}_j.$$

Therefore, $\mathcal{J}_j$ is a prime (maximal) ideal in $\mathcal{P}$. And from the previous argument, each zero of $\mathcal{J}_j$ is also a zero of $\mathcal{I}$ (a solution of the system $\mathcal{S}$) with multiplicity e_j.

Let $\mathcal{I}_j$ be the ideal $(\mathcal{I}, (H_{Y,j}(a_1x_1 + \cdots + a_nx_n))^{e'_j})$, where e'_j is the multiplicity of $H_{Y,j}$ as a factor of M_Y, and $\mathcal{I}_j^0$ be the ideal $(\mathcal{I}, H_{Y,j}(a_1x_1 + \cdots + a_nx_n))$. Moreover, let $\mathcal{I}^0$ be the ideal $(\mathcal{I}, h_Y)$.

By the above argument, we have now the following facts which correspond to a primary decomposition in Gianni *et al.* (1988).

COROLLARY 3.6.

(1) *The ideals $\mathcal{I}_j$ and $\mathcal{I}_j^0$ are $\mathcal{J}_j$-primary ideals.*
(2) *A decomposition $\mathcal{I} = \mathcal{I}_1 \cap \cdots \cap \mathcal{I}_s$ gives the irredundant primary decomposition of $\mathcal{I}$.*
(3) *The set of all zeros of $\mathcal{I}_i$ with multiplicities counted coincides with $\mathcal{V}_i$ and the multiplicity of each zero of $\mathcal{I}_i$ coincides with e_i for $i = 1, \ldots, s$.*
(4) *For each j, the ideal $(\mathcal{I}, h_1(x_1), \ldots, h_n(x_n), H_{Y,j}(a_1x_1 + \cdots + a_nx_n))$ coincides with the prime ideal $\mathcal{J}_j$.*

3.2. FURTHER PROPERTIES OF THE RADICAL AND THE PRIMARY DECOMPOSITION

Here, we continue the study of the subject in the previous subsection.

THEOREM 3.7. *Let e be the largest integer among $e_1, \ldots, e_s$. Then, for every polynomial $G(x_1, \ldots, x_n)$ belonging to the radical of $\mathcal{I}$, $G(x_1, \ldots, x_n)^e$ belongs to $\mathcal{I}$.*

PROOF. Consider the linear map $G(X_1, \ldots, X_n)$ on the residue class ring $\mathcal{A}_C$. By Lemma 2.7 and the fact that $G(X_1, \ldots, X_n)$ is nilpotent on $\mathcal{A}_C$, the matrix representation of $G(X_1, \ldots, X_n)$ with respect to the basis B' is expressed as

$$\mathrm{M}_{B'}(G(X_1, \ldots, X_n)) = \begin{pmatrix} \mathrm{N}_1 & 0 & \cdots & 0 \\ 0 & \mathrm{N}_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \mathrm{N}_{\ell'} \end{pmatrix},$$

where N_k is a nilpotent matrix for $k = 1, ..., \ell'$. By Lemma 2.7, each block N_k corresponds with one zero of the ideal $\mathcal{I}$ and the dimension of N_k coincides with the multiplicity of the corresponding zero. Thus, for each block N_k, we have $(\mathrm{N}_k)^e = 0$. This implies that $G(X_1, ..., X_n)^e$ vanishes on $\mathcal{A}_C$ and also on $\mathcal{A}$. Thus, $G(x_1, ..., x_n)^e$ belongs to $\mathcal{I}$. □

By Theorem 3.7, we can improve Theorem 3.4.

COROLLARY 3.8. *For each i, $(x_i - \beta_i(a_1x_1 + \cdots + a_nx_n))^e$ belongs to $\mathcal{I}$. For each i and j, $(x_i - \beta_{i,j}(a_1x_1 + \cdots + a_nx_n))^{e_j}$ belongs to $\mathcal{I}_j$ and $\mathcal{I}_j^0$.*

From now on, we denote $a_1x_1 + \cdots + a_nx_n$ by y. For each i, we denote by m_i the smallest integer such that $(x_i - \beta_i(y))^{m_i}$ belongs to $\mathcal{I}$. Moreover, we denote by m_i^0 the smallest integer such that $(x_i - \beta_i(y))^{m_i^0}$ belongs to $\mathcal{I}^0$, by $m_{i,j}$ the smallest integer such that $(x_i - \beta_{i,j}(y))^{m_{i,j}}$ belongs to $\mathcal{I}_j$, and by $m_{i,j}^0$ the smallest integer such that $(x_i - \beta_{i,j}(y))^{m_{i,j}^0}$ belongs to $\mathcal{I}_j^0$. Then, $m_{i,j} \geq m_{i,j}^0$. By the Chinese remainder theorem, $(x_i - \beta_i(y))^m \equiv (x_i - \beta_{i,j}(y))^m \bmod H_{Y,j}(y)$ for a positive integer m. From this and the primary decomposition, we have

LEMMA 3.9. *$m_i = \max\{m_{i,1}, ..., m_{i,s}\}$ and $m_i^0 = \max\{m_{i,1}^0, ..., m_{i,s}^0\}$.*

DEFINITION 3.2. Let H be a factor of H_Y over $\mathbb{Q}$. Consider a bivariate polynomial $G(u_1, u_2)$ such that $G(x_i, y)$ belongs to the ideal $(\mathcal{I}, H)$. We call $G(u_1, u_2)$ a *minimal polynomial of x_i with respect to y in $(\mathcal{I}, H)$*, if $G(u_1, u_2)$ is monic with respect to u_1 and it has minimal degree with respect to u_1 among all polynomials $\tilde{G}(u_1, u_2)$ in $(\mathcal{I}, H)$ which are monic with respect to u_1.

THEOREM 3.10. *For a bivariate polynomial $G(u_1, u_2)$ over $\mathbb{Q}$, $G(u_1, u_2)$ is divisible by $(u_1 - \beta_{i,j}(u_2))^{m_{i,j}^0}$ modulo $H_{Y,j}(u_2)$ if and only if $G(x_i, y)$ belongs to $\mathcal{I}_j^0$. Thus, a minimal polynomial of x_i with respect to y in $\mathcal{I}_j^0$ coincides with $(x_i - \beta_{i,j}(y))^{m_{i,j}^0}$ modulo $H_{Y,j}(y)$, and so its coefficient of $x_i^{m_{i,j}^0 - 1}$ coincides with $(-1) \cdot m_{i,j}^0 \cdot \beta_{i,j}(y)$ modulo $H_{Y,j}(y)$.*

PROOF. Let $G(u_1, u_2)$ be a bivariate polynomial over $\mathbb{Q}$ which belongs to $\mathcal{I}_j^0$. Consider the restrictions of linear maps X_i on the residue class ring $\mathcal{P}_C/(\mathcal{I}_j^0)_C$, which we also denote by the same symbols X_i. Take a suitable base B' of $\mathcal{P}_C/(\mathcal{I}_j^0)_C$ for upper triangularization of all X_i. Since $G(x_i, y)$ belongs to $\mathcal{I}_j^0$, $G(X_i, Y)$ vanishes. Since each diagonal component of $\mathrm{M}_{B'}(G(X_i, Y))$ is $G(\alpha_{i,k}, a(\alpha_k))$, $G(\alpha_{i,k}, a(\alpha_k)) = 0$ for every $\alpha_k \in \mathcal{V}_j$. From this and the fact that $\mathbb{Q}[y]/(H_{Y,j}(y)) \cong \mathbb{Q}(a(\alpha_k))$, it follows that $G(x_i, y) \equiv 0$ or $G(x_i, y)$ has $(x_i - \beta_{i,j}(y))$ as a factor over $\mathbb{Q}[x_i, y]/(H_{Y,j}(y))$. If $G(x_i, y) \equiv 0$ over $\mathbb{Q}[x_i, y]/(H_{Y,j}(y))$, then the statement is true. Suppose that $G(x_i, y) \not\equiv 0$ and $G(x_i, y)$ is divisible by $(x_i - \beta_{i,j}(y))^m$ but not divisible by $(x_i - \beta_{i,j}(y))^{m+1}$ over $\mathbb{Q}[x_i, y]/(H_{Y,j}(y))$. Then,

$$G(x_i, y) = (x_i - \beta_{i,j}(y))^m \cdot G_1(x_i, y) + H_{Y,j}(y) \cdot L(x_i, y),$$

where $G_1(x_i, y), L(x_i, y) \in \mathbb{Q}[x_i, y]$. From this,

$$0 = G(X_i, Y) = (X_i - \beta_{i,j}(Y))^m \cdot G_1(X_i, Y) \text{ in } END(\mathcal{P}_C/(\mathcal{I}_j^0)_C).$$

If $(X_i - \beta_{i,j}(Y))^m \neq 0$, then $G_1(X_i, Y)$ is a degenerate map. By seeing the diagonal components of the matrix representation of $G_1(X_i, Y)$, there is some α_k in $\mathcal{V}_j$ such that $G_1(\alpha_{i,k}, a(\alpha_k)) = 0$. Since all $a(\alpha_k)$, where $\alpha_k \in \mathcal{V}_j$, are algebraic conjugates over $\mathbb{Q}$, we have $G_1(\alpha_{i,k}, a(\alpha_k)) = 0$ for every $\alpha_k \in \mathcal{V}_j$. Then, it follows that $G_1(x_i, y)$ has $(x_i - \beta_{i,j}(y))$ as a factor in $\mathbb{Q}[x_i, y]/(H_{Y,j}(y))$ and this is a contradiction. Thus, $(X_i - \beta_{i,j}(Y))^m = 0$ and so $(x_i - \beta_{i,j}(y))^m$ belongs to $\mathcal{I}_j^0$. Hence $m \geq m_{i,j}^0$.

Conversely, if $G(u_1, u_2)$ is divisible by $(u_1 - \beta_{i,j}(u_2))^{m_{i,j}^0}$ modulo $H_{Y,j}(u_2)$, then $G(u_1, u_2)$ can be expressed as

$$G(u_1, u_2) = D(u_1, u_2)(u_1 - \beta_{i,j}(u_2))^{m_{i,j}^0} + E(u_1, u_2)H_{Y,j}(u_2),$$

where $D(u_1, u_2), E(u_1, u_2) \in \mathbb{Q}[u_1, u_2]$. Since $(x_i - \beta_{i,j}(y))^{m_{i,j}^0}$ and $H_{Y,j}(y)$ belong to $\mathcal{I}_j^0$, $G(x_i, a_1 x_1 + \cdots + a_n x_n)$ also belongs to $\mathcal{I}_j^0$. □

By Theorem 3.10 and the primary decomposition, we also have the following.

COROLLARY 3.11. *Let H be a factor of h_Y and $G(u_1, u_2)$ be a bivariate polynomial over $\mathbb{Q}$. Then, $G(u_1, u_2)$ is divisible by $(u_1 - \beta_{i,j}(u_2))^{m_{i,j}^0}$ modulo $H_{Y,j}(u_2)$ for every j such that $H_{Y,j}$ is a factor of H, if and only if $G(x_i, y)$ belongs to the ideal $(\mathcal{I}, H)$. Since a minimal polynomial of x_i with respect to y in $(\mathcal{I}, H)$ is constructed from $(x_i - \beta_{i,j}(y))^{m_{i,j}^0}$ by the Chinese remainder theorem, the degree of a minimal polynomial coincides with the largest $m_{i,j}^0$ among all j such that $H_{Y,j}$ is a factor of H.*

REMARK 3.1. As for multiplicities, we obtain the following results by considering Jordan's normal forms of the matrix representation of Y.

PROPOSITION 3.12. *The multiplicity of each zero of $\mathcal{I}_j$ is e_j, and that of $\mathcal{I}_j^0$ is at most $e_j - e_j' + 1$. If $e_j = e_j'$, then the ideal $\mathcal{I}_j^0$ coincides with its associated prime ideal $\mathcal{J}_j$. Consequently, in this case, each zero of $\mathcal{I}_j^0$ has the multiplicity e_j as a solution of S.*

3.3. LINEAR COORDINATE TRANSFORMATION AND BASIS CONVERSION

The results in Section 3.1, 3.2 are closely related to linear coordinate transformations into "general position" and expressing solutions as $x_i = \beta_i(y)$, $i = 1, ..., n$, where y ranges over all roots of a certain polynomial. And this expression is related to a Gröbner basis of the radical of the given ideal. First we define necessary notions.

DEFINITION 3.3. For an element $a = (a_1, ..., a_n)$ with $a_n \neq 0$ in $\mathbb{Z}^n$, we define a linear coordinate transformation ϕ_a which transforms the coordinates $x_1, ..., x_n$ to $z_1, ..., z_n$ as follows;

$$z_1 = x_1, ..., z_{n-1} = x_{n-1}, \text{ and } z_n = a_1 x_1 + \cdots + a_n x_n.$$

DEFINITION 3.4. If the reduced Gröbner base $\mathcal{G}$ of the ideal $\mathcal{I}$ under the lexicographic order $x_1 > x_2 > ... > x_n$ has the form

$$\{x_1 - \beta_1(x_n), ..., x_{n-1} - \beta_{n-1}(x_n), H(x_n)\},$$

we say that *the form of $\mathcal{G}$ is simple and $\mathcal{I}$ has a Gröbner basis in simple form.* Moreover, if after the linear coordinate transformation ϕ_a defined by a vector a with $a_n \neq 0$ the reduced Gröbner basis of the transformed ideal $\bar{\mathcal{I}}$ under the lexicographic order has simple form, we say that *the vector a gives a Gröbner basis in simple form.*

Fix a sufficient vector a with $a_n \neq 0$ and consider the ideal $\bar{\mathcal{I}}$ transformed from $\mathcal{I}$ by the linear transformation ϕ_a. We also define the linear maps $Z_1,...,Z_n$. Then, from the previous subsections, the followings hold.

(i) Let H_{Z_i} and M_{Z_i} be the characteristic polynomial and the minimal polynomial of Z_i respectively. Then, $H_{Z_i} = H_{X_i}$, $M_{Z_i} = M_{X_i}$ for $i = 1,...,n-1$ and $H_{Z_n} = H_Y$ and $M_{Z_n} = M_Y$. We denote the irreducible factor $H_{Y,j}$ of H_{Z_n} by H_j for $j = 1,...,s$. Then the square free part of H_{Z_n} coincides with $h_Y = H_1 \cdots H_s$.

(ii) The radical $\sqrt{\bar{\mathcal{I}}}$ contains the polynomials $z_i - \beta_i(z_n)$, $i = 1,...,n-1$, and $h_Y(z_n)$, all of which form its Gröbner basis in simple form under the lexicographic order $z_1 > z_2 > ... > z_n$. (This shows Proposition 2.2 in Kobayashi *et al.*, 1989.)

(iii) By letting $\bar{\mathcal{I}}_j = (\bar{\mathcal{I}}, (H_j)^{e_j}(z_n))$, a decomposition $\bar{\mathcal{I}} = \bar{\mathcal{I}}_1 \cap \cdots \cap \bar{\mathcal{I}}_s$ gives the irredundant primary decomposition of $\bar{\mathcal{I}}$. The associated prime $\bar{\mathcal{J}}_j$ of $\bar{\mathcal{I}}_j$ contains $z_i - \beta_{i,j}(z_n)$, $i = 1,...,n-1$, and $H_j(z_n)$, all of which form its Gröbner basis in simple form under the lexicographic order $z_1 > z_2 > ... > z_n$. Each zero of $\bar{\mathcal{J}}_j$ has the multiplicity e_j as a zero of $\bar{\mathcal{I}}_j$.

(iv) For $\bar{\mathcal{I}}_j^0 = (\bar{\mathcal{I}}, H_j)$, $(z_i - \beta_{i,j}(z_n))^{m^0_{i,j}}$ is the minimal polynomial of z_i with respect to z_n in the ideal $\bar{\mathcal{I}}_j^0$. (This is an extension of Proposition 3.1 in Kobayashi *et al.*, 1989.)

REMARK 3.2. According to Definition 7.2 in Gianni *et al.* (1988), the ideal $\bar{\mathcal{I}}$ is *in general position.* In their paper, they discussed how to put the given ideal in general position, and they showed that it can be done by simply applying a linear coordinate transformation, which is nothing but the one defined by a sufficient vector.

REMARK 3.3. We remark that in the case where $\mathcal{I}$ does not coincide with its radical but has a Gröbner basis in simple form after a suitable linear coordinate transformation, almost every vector gives a Gröbner basis in simple form the same as in the case where the ideal coincides with its radical. Now assume that $\mathcal{I} \neq \sqrt{\mathcal{I}}$.

LEMMA 3.13. *A sufficient vector $a = (a_1,...,a_n)$ with $a_n \neq 0$ gives a Gröbner base in simple form if and only if the minimal polynomial of $Z_n = a_1X_1 + \cdots + a_nX_n$ coincides with the characteristic polynomial of Z_n.*

PROOF. By considering the dimension of the residue class ring $\mathcal{A}$, the transformed ideal has a Gröbner base in simple form if and only if $\{1, z_n, z_n^2, ..., z_n^{\ell-1}\}$ becomes a basis of the residue class ring. And $\{1, z_n, z_n^2, ..., z_n^{\ell-1}\}$ becomes a basis if and only if the minimal polynomial of Z_n coincides with the characteristic polynomial of Z_n. □

Let $\beta_1,...,\beta_{\ell'}$ be all distinct zeros of $\mathcal{I}$ and let E_i be the multiplicity of β_i for $i = 1,...,\ell'$. To each $\beta_i = (\beta_{1,i},...,\beta_{n,i})$, $i = 1,...,\ell'$, an $\mathcal{X}$-invariant subspace W_i with dimension E_i associates. Moreover, there is a tower of subspaces

$$W_i^{(0)} = \{0\} \subset W_i^{(1)} \subset \cdots \subset W_i^{(t_i)} = W_i,$$

where $W_i^{(k)}/W_i^{(k-1)}$ is the intersection of the kernels of the linear maps $(X_j - \beta_{j,i}I)$ on $W_i/W_i^{(k-1)}$ for $k = 1, ..., t_i$. Then we have:

> A vector a gives a Gröbner basis in simple form if and only if the nilpotent linear map $(Z_n - a(\beta_i)I)^{E_i-1} \neq 0$ on W_i for every i.

Since Z_n acts each factor space $\tilde{W}_i^{(k)} = W_i^{(k)}/W_i^{(k-1)}$, $k = 1, ..., t_i$ and $Z_n \equiv a(\beta_i)I$ on $\tilde{W}_i^{(k)}$, the above condition is equivalent to the following:

$$t_i = E_i \text{ and } (Z_n - a(\beta_i)I)W_i^{(k)} \not\subset W_i^{(k-2)} \text{ for every } i \text{ and } k.$$

From these formulas, we can construct finitely many non-trivial linear equations such that if a sufficient vector a does not satisfy any of those, then a gives a Gröbner base in simple form. Since the sufficiency of a is also verified if a does not satisfy finitely many number of linear equations, see Section 4.2, we can state that if there is a sufficient vector which gives a Gröbner base in simple form, then almost every vector also does.

THEOREM 3.14. *If there is a vector which gives a Gröbner basis in simple form, then almost every vector gives a Gröbner basis in simple form.*

4. Construction of the Solutions in Simple Form

We show an application of the results in Section 3 for the computation of solutions of systems. For actual computations, there are many way to describe the solutions. Here we concentrate on giving all solutions of the given system in the following form:

$$(\beta_1(\theta), ..., \beta_{n-1}(\theta), \beta_n(\theta)),$$

where θ ranges over all roots of a certain univariate polynomial. Here we say that the above form of the solutions is *simple*. Discussion on the above form of solutions is given first in Kobayashi *et al.* (1988, 1989), where they proved that for "almost every" system with finitely many solutions, after a suitable linear coordinate transformation $x_1, ..., x_n$ to $z_1, ..., z_n$, the reduced Gröbner basis of the transformed ideal will be in the following simple form:

$$\{z_1 - \beta_1(z_n), ..., z_{n-1} - \beta_{n-1}(z_n), \beta_n(z_n)\}.$$

Their method is only applicable for the case where the ideal generated by the given system coincides with its radical. In Kobayashi *et al.* (1988, 1989) they presented another method for the case where the ideal generated by the given system does not coincide with its radical. But in the worst case, their method for the non-radical case needs the constructions of Gröbner bases $(n-1)$-times for each primary ideal in the primary decomposition of the given ideal. The new methods presented here are applicable even for the non-radical case, and thus they *reduce* unnecessary constructions of Gröbner bases.

4.1. IMPROVED METHODS FOR KOBAYASHI *et al.*'S ALGORITHMS

We show several improved methods for Kobayashi *et al.* (1988, 1989). Their method has a probabilistic nature in finding a *general position*. Thus, we assume that we have

already known a sufficient vector a with $a_n \neq 0$. In their method, before calculating a Gröbner basis of the ideal $\mathcal{I}$, we execute the linear coordinate transformation ϕ_a on $\mathcal{P}$ defined by a, which transforms the coordinates $x_1, ..., x_n$ to $z_1, ..., z_n$ as follows;

$$z_1 = x_1, ..., z_{n-1} = x_{n-1} \text{ and } z_n = a_1 x_1 + \cdots + a_n x_n.$$

Let $\bar{\mathcal{I}}$ be the transformed ideal. After transforming the coordinates, the following steps are executed;

(S1) calculate the reduced Gröbner basis of the ideal $\bar{\mathcal{I}}$ under the total degree order,
(S2) calculate the minimal polynomial M_{Z_n} of Z_n by solving linear equations, (see Method 6.11 in Buchberger, 1985 or Algorithm 2.2 in Kobayashi *et al.*, 1988),
(S3) factorize M_{Z_n} into its irreducible factors $H_{Y,1}, ..., H_{Y,s}$ over $\mathbb{Q}$.

Then, we have the ideals $\bar{\mathcal{I}}_k^0 = (\bar{\mathcal{I}}, H_{Y,k}(z_n))$. For simplicity, let $H_k(z_n) = H_{Y,k}(z_n)$.

An algorithm without additional constructions of gröbner bases

After the above steps, all solutions in simple form are constructed by Algorithm 3 in Kobayashi *et al.* (1989). By Theorem 3.10, we can improve their algorithm as follows:

ALGORITHM 1. (algorithm for a 0-dimensional primary ideal)
Input: a Gröbner basis $\bar{\mathcal{G}}$ of $\bar{\mathcal{I}}$, an irreducible factor H_k of the minimal polynomial M_{Z_n} of Z_n (after the steps (S1), (S2) and (S3));
Output: all zeros of the ideal $(\bar{\mathcal{I}}, H_k(z_n))$ in the form $(G_1(z_n), ..., G_{n-1}(z_n), z_n)$ where z_n ranges over all roots of H_k;

(1): for i:=1 to $n-1$ do;
  (1.1): compute the minimal polynomial $G(z_i, z_n)$ of z_i with respect to z_n in the ideal $(\bar{\mathcal{I}}, H_k(z_n))$ by Algorithm 2;
  (1.2): $G_i(z_n)$:=$g(z_n)/j$, where $G(z_i, z_n) = z_i^j - g(z_n) z_i^{j-1} + \cdots$;
(2): return $(G_1(z_n), ..., G_{n-1}(z_n), z_n)$.

Algorithm 2 is obtained by modifying existing algorithms such as Buchberger (1985), Kobayashi *et al.* (1988, 1989) or Lazard (1992). We note that a polynomial g lies in the ideal $(\bar{\mathcal{I}}, H)$ if and only if g lies in $H(Z_n)(\mathcal{P}/\bar{\mathcal{I}})$ as an element in $(\mathcal{P}/\bar{\mathcal{I}})$ by Lemma 2.3.

ALGORITHM 2. (algorithm for the minimal polynomial of z_i with respect to z_n)
Input: a Gröbner basis $\bar{\mathcal{G}}$ of $\bar{\mathcal{I}}$, a factor H of M_Y and an index i;
Output: the minimal polynomial of z_i with respect to z_n in the ideal $(\bar{\mathcal{I}}, H)$;

(0): compute a basis B of the residue class ring $\mathcal{P}/\bar{\mathcal{I}}$ such that $B = B_1 \cup B_2$, where B_1 is a basis of the image of $H(Z_n)$ on $\mathcal{P}/\bar{\mathcal{I}}$;
  (from this, we define the projection ϕ of $\mathcal{P}/\bar{\mathcal{I}}$ to $\mathcal{P}/(\bar{\mathcal{I}}, H)$);
(1): j:=0;
(2): for r:=0 to $m-1$, where m =degree H, do;
  $p_{j,r} = \phi(NormalForm((z_i)^j (z_n)^r))$;
(3): solve the equation $p_{j,0} + \sum_{0 \leq r < j, 0 \leq t < m} d_{r,t} p_{r,t} = 0$ for $d_{r,t}$ over $\mathbb{Q}$;
  if there is no solution, then j:=$j+1$ and go to step (2);
(4): $G(z_i, z_n) = z_i^j + \sum_{0 \leq r < j, 0 \leq t < m} d_{r,t} z_i^r z_n^t$;
(5): return G.

REMARK 4.1. By Corollary 3.6, we get the multiplicities of the solutions as the multiplicities e_j of factors $H_{Y,j}$ in H_Y. (We note that for an $\ell \times \ell$ matrix the characteristic polynomial can be calculated efficiently in $O(\ell^3)$ time complexity by Danilevski's method.) Also by Corollary 3.8, the solution is found at $j \leq e$ in Algorithm 2.

An algorithm without factorization

As another improvement, we present a method by which we can avoid (S3), the step of factorization.

Let $H_{(0)}(z_n)$ be the square free part of the minimal polynomial of Z_n, i.e., $H_{(0)}(z_n) = H_1(z_n)\cdots H_s(z_n)$, and let $H^{(0)} = 1$. $H_{(0)}(z_n)$ can be computed only by GCD computation.

PROCEDURE. We repeat the following process from $j = 0$ until $H_{(j+1)} = 1$;

(i) compute the minimal polynomial $G^{(j)}(z_i, z_n)$ of z_i with respect to z_n in $(\bar{\mathcal{I}}, H_{(j)}(z_n))$,

(ii) compute $H^{(j+1)}(z_n) = \mathrm{GCD}(G^{(j)}(z_i, z_n) - (z_i - g^{(j)}(z_n)/m_i^{(j)})^{m_i^{(j)}}, H_{(j)}(z_n))$, where $G^{(j)}(z_i, z_n) = z_i^{m_i^{(j)}} - g^{(j)}(z_n) z_i^{m_i^{(j)}-1} + \cdots$, and

(iii) compute the cofactor $H_{(j+1)}(z_n) = H_{(j)}(z_n)/H^{(j+1)}(z_n)$.

THEOREM 4.1. *The above process terminates in at most s steps. Moreover, for each j-th step we have $g^{(j)}(z_n)/m_i^{(j)} \equiv \beta_i(z_n)$ mod $H^{(j+1)}(z_n)$.*

PROOF. By combining Theorem 3.10 and the Chinese remainder theorem, it follows that $g^{(j)}(z_n)/m_i^{(j)} \equiv \beta_i(z_n) \bmod H^{(j+1)}(z_n)$ for each j. Thus, we show the termination of the procedure. By Corollary 3.11 for the ideal $(\bar{\mathcal{I}}, H_{(j)})$, there is some factor H_k of $H_{(j)}$ such that

$$G^{(j)}(z_i, z_n) \equiv (z_i - \beta_{i,k}(z_n))^{m_i^{(j)}} \bmod H_k(z_n).$$

This implies that $H_{(j+1)} \neq H_{(j)}$. This guarantees the termination of the procedure at most s, the number of irreducible factors, steps. □

Once the procedure terminates, by the Chinese remainder theorem, we can construct $\beta_i(z_n)$ by $g^{(j)}$'s. Thus, we have the following algorithm without factorization but GCD computation.

ALGORITHM 3. (algorithm for a 0-dimensional ideal without factorization)
Input: a reduced Gröbner basis $\bar{\mathcal{G}}$ of $\bar{\mathcal{I}}$ (after the Steps (S1) and (S2));
Output: all zeros of the ideal $\bar{\mathcal{I}}$ in the form $(G_1(z_n), \ldots, G_{n-1}(z_n), z_n)$ where z_n ranges over all roots of $H_{(0)}$;

(1): M_{Z_n} := the minimal polynomial of Z_n;
  $H_{(0)}$:= the square free part of M_{Z_n};
(2): for $i = 1$ to $n-1$ do;
  (2.1): $j = 0$;
  (2.2): while $H_{(j)} \neq 1$ do;
    (a): $G^{(j)}(z_i, z_n)$:= the minimal polynomial of z_i
      with respect to z_n in $(\bar{\mathcal{I}}, H_{(j)}(z_n))$;
    (b): $m_i^{(j)}$:=degree$_{z_i}$ $G^{(j)}(z_i, z_n)$;

$g^{(j)}$:= the coefficient of $z_i^{m_i^{(j)}-1}$ in $(-1)\cdot G^{(j)}(z_i, z_n)$;
(c): $H^{(j+1)}(z_n)$:=GCD$(G^{(j)}(z_i, z_n) - (z_i - g^{(j)}(z_n)/m_i^{(j)})^{m_i^{(j)}}, H_{(j)}(z_n))$;
$H_{(j+1)}(z_n) := H_{(j)}(z_n)/H^{(j+1)}(z_n)$;
(d): $j := j + 1$;
(2.3): construct $G_i(z_n)$ by the Chinese remainder theorem from $g^{(j)}/m_i^{(j)}$'s;
(3): return $G_1,...,G_{n-1}$ and $H_{(0)}$.

An algorithm without transforming coordinates

Of course, we can solve the solutions of the system without transforming the coordinates actually. Since Algorithm 2 and Algorithm 3 use solving linear equations and GCD computation of polynomials, we can modify Algorithm 3 to the following algorithm without transforming the coordinates. Since coordinate transformations usually generate dense polynomials, avoiding coordinate transformations will improve the actual efficiency.

ALGORITHM 4. (algorithm for 0-dimensional ideal without coordinate transformation)
Input: polynomials in the system $\mathcal{S}$ and a sufficient vector a;
Output: all solutions of the system $\mathcal{S}$ in the form $(G_1(z), ..., G_n(z))$ where z ranges over all roots of a certain univariate polynomial $h(z)$;

(1): calculate the reduced Gröbner basis of the ideal $\mathcal{I}$;
(2): calculate the linear map $Z = a_1X_1 + \cdots a_nX_n$ by using the basis of the residue class ring $\mathcal{P}/\mathcal{I}$ obtained from the Gröbner basis, and also calculate the minimal polynomial and the characteristic polynomial of Z;
(3): apply Algorithm 3, where $z_1 = x_1,...,z_{n-1} = x_{n-1}$ and $z_n = a_1x_1 + \cdots + a_nx_n$;
(4): return $G_1, ..., G_n$, where $G_n(t) = (t - a_1G_1(t) - \cdots - a_{n-1}G_{n-1}(t))/a_n$, and h as the square free part of the minimal polynomial of Z.

4.2. DETERMINISTIC METHODS FOR SOLVING ALL SOLUTIONS

Now we consider the case where we do not have a sufficient vector a. Although almost every vector is a sufficient vector, to get a complete algorithm we have to deal with the choice of such vectors and resolve its probabilistic feature. There are two ways: One way is to choose a vector a randomly and to employ the whole method presented above until we get a sufficient vector and the correct solutions; the other way is previously computing the radical of given ideal and testing the sufficiency of randomly chosen vectors a by the square freeness of the minimal polynomial of $a(X)$ based on Lemma 3.13.

Thus, the important problem of deterministic methods is the bound of the number of necessary trials. We discuss how many trials are needed to obtain a sufficient vector. As an efficient way for trials, we employ n-base trial described in Yokoyama *et al.* (1989b).

DEFINITION 4.1. Let S be a subset of $\mathbb{Z}^n$. S is called an n-base set, if any distinct n elements of S are linearly independent over $\mathbb{Q}$.

Zippel (1990) also defined the same notion and called it a *maximally independent set.* We can construct an n-base set with any cardinality in terms of integer parameters. For example, $S = \{(1, u, u^2, ..., u^{n-1}) | u \in \mathbb{Z}\}$ is an n-base set with infinitely many elements. Moreover, according to Zippel (1990), for a positive integer t, $S_t = \{(1, u \bmod p, u^2 \bmod p, ..., u^{n-1} \bmod p) | u = 1, ..., t\}$, where p is the smallest prime larger than t, is also an n-base

set with t elements. Since there is a prime between t and $2t$, the absolute values of all elements in S_t are bounded by $2t$.

Then the number of trials is bounded by the following manner. Here, we use the same notation as in Section 3. Therefore, s is the number of distinct associated prime ideals $\mathcal{J}_j$, ℓ' is the number of distinct zeros of $\mathcal{I}$ and ℓ is the number of zeros of $\mathcal{I}$ with multiplicities counted.

THEOREM 4.2. *Let T be an n-base set with t elements, where $t = s(\ell' - 1)(n-1) + 1$, such that every element in T has non zero n-th component. Then, there is an element a in T which is a sufficient vector. Thus, the number of trial is bounded by t.*

PROOF. For an element a in $\mathbb{Z}^n$, a is a sufficient vector if $a(\alpha_k) \neq a(\alpha_j)$ for $\alpha_k \neq \alpha_j$. Let $\mathcal{V}' = \{\beta_1, ..., \beta_{\ell'}\}$ be the set of all distinct solutions in $\mathcal{V}$, and β_{k_i} be an element in $\mathcal{V}_i$. Since algebraic conjugates of elements of $\mathcal{V}$ also belong to $\mathcal{V}$, the Galois group of the Galois closure of $\mathbb{Q}(\alpha_{1,1}, ..., \alpha_{n,\ell})$ over $\mathbb{Q}$ acts on $\mathcal{V}$. By seeing this action, it follows that a is a sufficient vector if $a(\beta_{k_i}) \neq a(\beta_j)$ for $i = 1, ..., s$, $j = 1, ..., \ell'$ *and* $\beta_j \neq \beta_{k_i}$. Therefore, a is a sufficient vector if and only if a does not belong to the set of solutions of the equations $a(\beta_{k_i}) - a(\beta_j) = 0$ for any pair β_{k_i}, β_j, where $j \neq k_i$. Since there are $s(\ell' - 1)$ pairs to be tested and the set of solutions of each linear equation forms a submodule whose rank is at most $n-1$, we can show that in an n-base set consisting of at least $s(\ell' - 1)(n-1) + 1$ elements there exists an element a which does not belong to any of those submodules. Hence, in T there is a sufficient vector. □

By Bézout's theorem, ℓ is bounded by d^n, where d is the maximal total degree of polynomials in the system. From this, we also have the following.

$$t < s\ell' n \leq n d^{2n}.$$

This bound seems too large to explain the actual behavior. So tight bounds are needed. But the existence of a bound of numbers of trials guarantees the termination of algorithms employing n-base trial.

REMARK 4.2. Hintenaus (1989) used a similar method for finding a "generic point," and by this method, he constructed a deterministic algorithm for solving systems.

4.3. COMPLEXITY OF ALGORITHMS AND REMARKS

First we discuss on the complexity of the proposed algorithms; next we give a discussion on comparison of existing algorithms for solving systems.

Complexity of algorithms

The proposed algorithms in the previous subsections are designed for avoiding tedious computations of Gröbner basis. We provide Algorithm 1, Algorithm 3 as probabilistic algorithms and Algorithm 4 with n-base trial as a deterministic algorithm. Since the deterministic one has higher complexity than the probabilistic one, we focus on the complexity of the deterministic one. We will show that its complexity is polynomial in d^n under a slight additional condition, where d is the maximal total degree of the polynomial in the system and n is the number of variables.

Since the proposed algorithms need a Gröbner basis at the beginning, the total complexity of them depends on the part of computing a Gröbner basis. But once we obtain a Gröbner basis, in Algorithm 4, the subsequent procedures includes, as major parts, computation of normal forms of polynomials, solving linear equations, GCD-computation of polynomials, all of which can be executed in polynomial time in n, ℓ, and the number of elements of the Gröbner basis and the magnitude of the coefficients of elements of the Gröbner basis. By Bézout's theorem, $\ell \leq d^n$ and so the number of the elements of the Gröbner basis is bounded by nd^n (see Faugère *et al.*, 1989). Moreover, since the number of trials is bounded by nd^{2n}, the norms of randomly chosen vectors in n-base trial are bounded by $2nd^{2n}$ and so their magnitudes are bounded by $O(nlog(d))$ if we employ S_t as an n-base set of t elements. Thus, the complexity of all procedures except the computation of a Gröbner basis is polynomial in d^n and the magnitude of the coefficients of elements of the Gröbner basis. Especially, the number of arithmetic operations of all procedure except the computation of a Gröbner basis is polynomial in d^n.

On the other hand, according to Faugère *et al.* (1989) and Lazard (1992), for computing Gröbner basis, degree-reverse-lexicographical order is the best. And for this order, if the solutions are finite in number counting the solutions at infinity, its computation is polynomial time in d^n. This implies that the magnitude of the coefficients of the elements of the Gröbner basis with respect to any degree-reverse-lexicographical order is bounded by a polynomial in d^n.

Thus, we can say that the complexity of Algorithm 4 with n-base trial is polynomial in d^n, provided that the solutions are finite in number counting the solutions at infinity, and this shows the efficiency of the proposed algorithms.

Comparison with other algorithms

Now we give a comparison of the proposed algorithms and other algorithms for the problem. As mentioned before, the proposed algorithms are considered as improvements of Kobayashi *et al.*'s algorithm applicable even for non-radical case, and avoiding unnecessary computations of Gröbner bases implies that Algorithm 4 with n-base trial has much smaller complexity than them, even though Algorithm 4 with n-base trial is deterministic and even if Kobayashi *et al.*'s algorithm employs an efficient algorithm for Gröbner basis under the lexicographical order such as Faugère *et al.*'s algorithm.

The method used in the proposed algorithms is very similar to ones for basis conversion algorithms. (See Faugère *et al.*, 1989.) The aim of basis conversion is to reduce a difficult problem, such as a computation of a Gröbner basis under lexicographic order, to an easier problem, such as a computation of one under total degree order. So it is the same as the aim of our improvement. Moreover, since in some case the proposed algorithms may output not only solutions but also a Gröbner basis in simple form and in any case they output a Gröbner basis of the radical of the ideal generated by the input polynomials, they may be called a certain kind of basis conversion algorithms which computes a Gröbner basis under lexicographic order in general position.

The proposed algorithms have a weak point which all algorithms for computing Gröbner bases in simple form have. A generic change of variables (coordinate transformation by a sufficient vector) may destroy the sparsity of the input polynomials, and it may also causes the growth of their coefficients. Moreover, the proposed algorithms need some extra computations, factorization of polynomials or GCD computation. But, even in other existing algorithms, if we want to express the solutions in simple form, we have to fac-

torize polynomials or compute GCD's of polynomials over algebraically extended fields. Then, one needs to find primitive elements of the algebraic extension fields, which is the same meaning as finding a sufficient vector, i.e., a generic change of variables. (For an example, see Procedure 7 in Lazard, 1992.) Thus, if we want to express the solutions in simple form, a generic change is unavoidable. From this, taking account of the fact that Algorithm 4 is polynomial in d^n, we believe that the proposed algorithms are efficient compared with other existing algorithms.

Acknowledgment

We are grateful to Professor B. Buchberger, Professor D. Lazard and Professor H. Kobayashi for reading an early version of this paper and giving us valuable and helpful comments. We are also indebted to the referee for many useful comments.

References

Auzinger, W., Stetter, H.J. (1989). An elimination algorithm for the computation of all zeros of a system of multivariate polynomial equations. Preprint.

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

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

Buchberger, B. (1988). Applications of Gröbner bases in non-linear computational geometry. *Springer Lecture Notes in Computer Science* **296**, 52–80.

Faugère, J.C., Gianni, P., Lazard, D., Mora, T. (1989). Efficient computation of zero-dimensional Gröbner bases by change of ordering. Technical Report of Laboratoire Informatique Theorique et Programmation (LITP) 89-52.

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

Hartshorne, R. (1977). *Algebraic Geometry*, Springer-Verlag.

Hintenaus, P. (1989). Decomposing and parameterizing the solution set of an algebraic system. Ph.D. Thesis, Johannes Kepler University, RISC-LINZ Report No. 89-27.

Kobayashi, H., Fujise, T., Furukawa, A. (1988). Solving systems of algebraic equations by a general elimination method. *J. Symbolic Computation* **5**, 303–320.

Kobayashi, H., Moritsugu S., Hogan, W. (1988). Solving systems of algebraic equations. Symbolic and Algebraic Computation, International Symposium ISSAC'88 (P. Gianni, ed.). *Springer Lecture Notes in Computer Science* **358**, 139–149.

Kobayashi, H., Moritsugu S., Hogan, W. (1989). On radical zero-dimensional ideals. *J. Symbolic Computation* **8**, 545-552.

Lazard, D. (1981). Résolution des systèmes d'équations algébriques. *Theor. Comp. Sci.* **15**, 77–110.

Lazard, D. (1983). Gröbner bases, Gaussian elimination and resolution of system of algebraic equations. Proc. EUROCAL '83. *Springer Lecture Notes in Computer Science* **162**, 146–156.

Lazard, D. (1992). Solving zero-dimensional algebraic systems. *J. Symbolic Computation* **13**, 117–131.

Seidenberg, A. (1974). Constructions in algebra. *Trans. Am. Math. Soc.* **197**, 273–313.

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

van der Waerden, B. L. (1936). *Moderne Algebra II*, Springer-Verlag.

van der Waerden, B. L. (1991). *Algebra II*, Springer-Verlag.

Yokoyama, K., Noro, M., Takeshima, T. (1989a). Solutions of systems of algebraic equations and linear maps on residue class rings. IIAS-SIS Research Report No. 94, FUJITSU LIMITED.

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

Yokoyama, K., Noro, M., Takeshima, T. (1990). Solutions of systems of algebraic equations and linear maps on residue class rings. IIAS-SIS Research Report No. 103, FUJITSU LIMITED.

Zariski, O., Samuel P. (1960). *Commutative Algebra II*, Springer-Verlag.

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