数式処理 *J.JSSAC (2000)*
Vol. 7, No. 4, pp. 2 - 22
論文

A Linear Algebra Method for Solving Systems of Algebraic Equations

Shuichi MORITSUGU
University of Library and Information Science*

Kazuko KURIYAMA
National Institute of Informatics †

(RECEIVED 1999/3/19 REVISED 2000/4/4)

Abstract

We consider the exact computation of matrix eigenproblems in residue class rings for solving systems of algebraic equations. We construct multiplication tables using a Gröbner basis of a zero-dimensional ideal. Then, we analyze the tables by exactly computing their Frobenius normal forms. The derogatoriness and the diagonalizability are determined by the normal forms, and the problem is divided into four cases:

(1) nonderogatory and diagonalizable case,
(2) nonderogatory and nondiagonalizable case,
(3) derogatory and diagonalizable case,
(4) derogatory and nondiagonalizable case.

Subsequently, we construct common eigenvectors symbolically, and compute all the exact zeros with their multiplicities. The result of empirical implementation is also shown.

1 Introduction

To solve a system of algebraic equations by computer algebra, the classical method of general elimination has been studied as the computation of Lazard's U-resultant [16][17]. Kobayashi *et al.* [14] showed an efficient algorithm for computing U-resultants by Gröbner bases of zero-dimensional ideals. Their method computes the matrices $A_{x_1}, \ldots, A_{x_s}$, which are nowadays called multiplication tables, and obtains the U-resultant as $\det(u_1 A_{x_1} + \cdots + u_s A_{x_s})$ with new indeterminates $u_1, \ldots, u_s$.

On the other hand, Auzinger and Stetter [1] proposed a method for computing the solutions of a system as the eigenvalues of certain matrices. At first they did not use

*moritsug@ulis.ac.jp
†kuriyama@nii.ac.jp

Gröbner bases, but in these years, multiplication tables $A_{x_1}, \ldots, A_{x_s}$ are usually computed by a Gröbner basis [25].

Stetter's method intends to solve matrix eigenproblems by numerical analysis technique. However, when the given polynomials have exact coefficients, the multiplication tables can be computed exactly through a Gröbner basis. Hence, we may apply symbolic computation technique to matrix eigenproblems. Takeshima and Yokoyama [27] proposed a symbolic method for computing the eigenvalues and the eigenvectors by Frobenius normal forms of matrices. Their method is very efficient because of avoiding arithmetic operations over an algebraic extension field. In this paper, we extend their idea and give the algorithms according to the properties of multiplication tables. Even though our exact computation method needs much more CPU-time than numerical methods such as [6][7], it is completely free from numerical errors. In particular, spurious multiple zeros, that is, simple zeros with the same x_i-coordinate, are exactly distinguished from genuine multiple zeros.

Our formulation gives the multiplicity of zeros at the same time as the computation of their location. Möller and Stetter [19][20][26] show that multiple zeros are characterized by the notion of *a dual basis* [18]. They consider a dual space and adopt a basis of differential conditions that describe the local behavior of multiple zeros. To the contrary, we show that it is enough for determining the location and the multiplicity of zeros to compute the Frobenius normal form of a matrix. The detail of our formulation on multiple zeros has been published as a separate paper [22].

We have implemented our method on the computer algebra system Reduce3.6 [12], and we report the result of the computation of several examples. Finally, we discuss the comparison with other methods and the efficiency of our method.

2 Basic Notions

2.1 Residue Class Ring and Multiplication Table

Let $I = (f_1, \ldots, f_\ell)$ be an ideal in a polynomial ring with rational number coefficients $R = \mathbf{Q}[x_1, \ldots, x_s]$. It is well-known that an ideal I is zero-dimensional if and only if the residue class ring R/I is finite-dimensional as a $\mathbf{Q}$-vector space. The following theorem is fundamental in the Gröbner basis theory [3][4].

Theorem 1 (Normal Set Basis)
Let G be a Gröbner basis of zero-dimensional ideal I with an arbitrary order. Then, the set of power products

$$B := \{x_1^{e_1} \cdots x_s^{e_s} \mid x_1^{e_1} \cdots x_s^{e_s} \textit{ is irreducible with } G\}$$

is a linearly independent basis for R/I as a $\mathbf{Q}$-vector space.

Let $B = \{t_1, \ldots, t_n\}$ be the normal set basis for R/I in the above theorem. Then, it is well-known that n coincides with the number of the zeros of I with their multiplicities counted. We define the multiplication tables A_{x_k} $(k = 1, \ldots, s)$ in R/I as follows.

Definition 2 (Multiplication Table for x_k)
Compute the normal form of the product of x_k and each t_i $(t_i \in B)$ with G:

$$x_k \cdot t_i \quad \mapsto \quad \sum_{j=1}^{n} a_{ij} \cdot t_j.$$

Then, the $n \times n$ matrix $A_{x_k} := [a_{ij}]$ is called the multiplication table for x_k in R/I.

Since we consider polynomials in $\mathbf{Q}[x_1, \ldots, x_s]$, the elements of A_{x_k} become rational numbers, namely, $a_{ij} \in \mathbf{Q}$.

The following fact is important for analyzing the family of multiplication tables $\{A_{x_k}\}$.

Lemma 3
The matrices A_{x_k}'s are commutative, that is, $A_{x_k} A_{x_\ell} = A_{x_\ell} A_{x_k}$ for every pair $(k, \ell = 1, \ldots, s)$.

Now we consider the problem of solving a system of algebraic equations

$$f_1(x_1, \ldots, x_s) = 0, \quad \ldots, \quad f_\ell(x_1, \ldots, x_s) = 0, \tag{1}$$

that is, the problem of finding all the zeros of an ideal $I = (f_1, \ldots, f_\ell)$. In this paper, we restrict ourselves to the case where I is zero-dimensional, namely, the system (1) has finitely many solutions. The relation between the zeros of I and the multiplication tables $\{A_{x_k}\}$ is elucidated by the following theorem [1][28]. Therefore, the problem of solving a system of algebraic equations is interpreted as a matrix eigenproblem.

Theorem 4 (Solutions by Matrix Eigenproblem)
Using one common regular matrix S, the commutative matrices $\{A_{x_k}\}$ are simultaneously transformed into upper triangular forms $U_k = S^{-1} A_{x_k} S$ $(k = 1, \ldots, s)$, where the diagonal elements of U_k are the eigenvalues of A_{x_k}. Let the diagonal elements of U_k be $u_{ii}^{(k)}$ $(i = 1, \ldots, n)$. Then, all the zeros of I, counting their multiplicities, coincide with $\left(u_{ii}^{(1)}, u_{ii}^{(2)}, \ldots, u_{ii}^{(s)}\right)$ $(i = 1, \ldots, n)$.

2.2 Frobenius Normal Form

In the following sections, we assume that the elements of a given matrix are rational numbers: $A = [a_{ij}]$, $a_{ij} \in \mathbf{Q}$. The following notions are well-known in the matrix theory.

Definition 5 (Companion Matrix)
The following $n \times n$ square matrix

$$C = \begin{bmatrix} 0 & 1 & & & \\ 0 & 0 & \ddots & & \text{O} \\ \vdots & \vdots & \ddots & \ddots & \\ 0 & 0 & \cdots & 0 & 1 \\ c_0 & c_1 & \cdots & c_{n-2} & c_{n-1} \end{bmatrix} \tag{2}$$

is called the companion matrix associated with the polynomial $f(x) = x^n - c_{n-1}x^{n-1} - \cdots - c_1 x - c_0$. In particular, the companion matrix associated with the first degree polynomial $f(x) = x - c_0$ is the 1×1 square matrix $[c_0]$.

Lemma 6
The characteristic polynomial $\varphi_C(x)$ and the minimal polynomial $\phi_C(x)$ of the companion matrix C are equal to $f(x)$.

Theorem 7 (Frobenius Normal Form)
Using a suitable regular matrix S, every $n \times n$ square matrix A can be transformed into the block diagonal matrix as follows:

$$F = S^{-1}AS = C_1 \oplus C_2 \oplus \cdots \oplus C_t. \tag{3}$$

It is called the Frobenius normal form (or the rational normal form) of A. Each block matrix $C_i (i = 1, \cdots, t)$ is an $m_i \times m_i$ companion matrix (2), and the associated polynomial $\varphi_{i+1}(x)$ of C_{i+1} divides the associated polynomial $\varphi_i(x)$ of C_i $(i = 1, \ldots, t-1)$. The matrix in the form (3) always exists and is uniquely determined for every given matrix. Moreover, the minimal polynomial $\phi_A(x)$ of A is equal to $\varphi_1(x)$, and the characteristic polynomial $\varphi_A(x)$ of A is given by $\varphi_1(x) \cdot \varphi_2(x) \cdots \varphi_t(x)$.

Danilevskii [8] showed the method for computing a block diagonal matrix like (3), but the result of his method did not necessarily satisfy the division condition

$$\varphi_t(x) \mid \varphi_{t-1}(x) \mid \cdots \mid \varphi_1(x),$$

hence his $\varphi_1(x)$ was not necessarily the minimal polynomial of A. However, the existence of strict meaning of the Frobenius normal form in Theorem 7 is shown in [11]. Our implementation is based on the algorithm given by [13], which eliminates the matrix elements like Gaussian elimination by computing similar transformation step by step: $\cdots S_3^{-1}\left(S_2^{-1}\left(S_1^{-1}AS_1\right)S_2\right)S_3\cdots$, and obtains F, S, S^{-1} in (3) finally.

Since Danilevskii's method is numerically unstable, it had been abandoned in the field of numerical analysis. However, on the assumption of exact computation, an efficient algorithm for the symbolic solution of matrix eigenproblems using Frobenius normal forms is proposed by [27]. The following lemmas are its straightforward extension.

Lemma 8 (Eigenvector of a Companion Matrix)
Let λ be an eigenvalue of an $n \times n$ companion matrix C (2) and we put a vector $\boldsymbol{u} := \left[1, \lambda, \lambda^2, \ldots, \lambda^{n-1}\right]^T$. Then, this vector $\boldsymbol{u}$ is an eigenvector of C with the eigenvalue λ.

Proof Since λ is a root of the characteristic polynomial $\varphi_C(x)$, we have

$$\varphi_C(\lambda) = \lambda^n - c_{n-1}\lambda^{n-1} - \cdots - c_1\lambda - c_0 = 0.$$

Then, we obtain

$$C\boldsymbol{u} = \begin{bmatrix} \lambda \\ \lambda^2 \\ \vdots \\ \lambda^{n-1} \\ c_0 + c_1\lambda + \cdots + c_{n-1}\lambda^{n-1} \end{bmatrix} = \begin{bmatrix} \lambda \\ \lambda^2 \\ \vdots \\ \lambda^{n-1} \\ \lambda^n \end{bmatrix} = \lambda\boldsymbol{u}.$$

∎

Note that, for the companion matrix C, there exists only one linearly independent eigenvector with the eigenvalue λ, even if λ is a multiple root of $\varphi_C(x)$.

Lemma 9 (Eigenvector of a Frobenius Normal Form)
Let λ be an eigenvalue of a Frobenius normal form F (3), and let $\varphi_i(x)$ be the associated polynomial of C_i ($i = 1, \ldots, t$). Suppose that λ satisfies $\varphi_1(\lambda) = \cdots = \varphi_k(\lambda) = 0$ and $\varphi_{k+1}(\lambda) \neq 0$ for some k. (When $k = t$, the last condition should be omitted.) For each block C_i with its size m_i, we put vectors $\tilde{\boldsymbol{u}}_i := \left[1, \lambda, \lambda^2, \ldots, \lambda^{m_i-1}\right]^T$ ($i = 1, \ldots, k$). Extending them to the vectors of size n, we put

$$\boldsymbol{u}_1 := \begin{bmatrix} \tilde{\boldsymbol{u}}_1 \\ \boldsymbol{0} \\ \vdots \\ \vdots \\ \boldsymbol{0} \end{bmatrix}, \quad \boldsymbol{u}_2 := \begin{bmatrix} \boldsymbol{0} \\ \tilde{\boldsymbol{u}}_2 \\ \boldsymbol{0} \\ \vdots \\ \boldsymbol{0} \end{bmatrix}, \quad \ldots, \quad \boldsymbol{u}_k := \begin{bmatrix} \boldsymbol{0} \\ \vdots \\ \boldsymbol{0} \\ \tilde{\boldsymbol{u}}_k \\ \boldsymbol{0} \end{bmatrix}, \tag{4}$$

where the size of each zero vector corresponds to each companion block. Then, these k vectors are eigenvectors of F with the eigenvalue λ.

Proof Apparently, the vectors $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k$ are linearly independent. According to Lemma 8, for each block C_i, we have $C_i\tilde{\boldsymbol{u}}_i = \lambda\tilde{\boldsymbol{u}}_i$ ($i = 1, \ldots, k$). Since the matrix F is block diagonal, it is easy to see that $F\boldsymbol{u}_i = \lambda\boldsymbol{u}_i$ ($i = 1, \ldots, k$). ∎

Note that this lemma gives also the dimension k of the eigenspace of F belonging to the eigenvalue λ, that is, k is determined to be such a number that $\varphi_1(\lambda) = \cdots = \varphi_k(\lambda) = 0$ and $\varphi_{k+1}(\lambda) \neq 0$.

Lemma 10 (Eigenvector of a General Matrix)
Let F be the Frobenius normal form of a matrix A, and $\boldsymbol{u}$ be one of the eigenvectors (4) *of F having λ as the eigenvalue. Then, λ is also the eigenvalue of A. The corresponding eigenvector of A is given by $\boldsymbol{v} := S\boldsymbol{u}$, where S is a similar transformation matrix such that $F = S^{-1}AS$* (3).

Proof Since A and F are similar, they have the same eigenvalues in common. Moreover, since we have $F\boldsymbol{u} = \lambda\boldsymbol{u}$ and $AS = SF$, we obtain

$$A\boldsymbol{v} = A(S\boldsymbol{u}) = (AS)\boldsymbol{u} = (SF)\boldsymbol{u} = S(F\boldsymbol{u}) = S(\lambda\boldsymbol{u}) = \lambda(S\boldsymbol{u}) = \lambda\boldsymbol{v}.$$

Therefore, $\boldsymbol{v}$ is an eigenvector of A having λ as the eigenvalue. ∎

The construction by the above lemmas does not require solving a system of linear equations $(A - \lambda E)\boldsymbol{x} = \mathbf{0}$ over an algebraic extension field $\mathbf{Q}(\lambda)$. We have only to reduce λ^ℓ in $\boldsymbol{u}$ by the definition polynomial of λ as shown in the later examples. Thus, symbolic expressions of eigenvalues and eigenvectors of a rational matrix can be efficiently computed.

2.3 Matrix Eigenproblem

When we consider a multiple eigenvalue of a matrix, we have to distinguish two kinds of multiplicities.

Definition 11 (Algebraic Multiplicity)
Let λ be an eigenvalue of a matrix A. If λ is a p-fold root of the characteristic polynomial $\varphi_A(x) = \det(A - xE)$, then it is called that λ has the algebraic multiplicity p.

Definition 12 (Geometric Multiplicity)
Let λ be an eigenvalue of a matrix A, and $V(\lambda, A)$ be the eigenspace of A belonging to λ. If the dimension of $V(\lambda, A)$ is m, then it is called that λ has the geometric multiplicity m.

Note that the inequality $m \leq p$ always holds between the both multiplicities. The following property of matrices is crucial in Stetter's method.

Definition 13 (Nonderogatoriness)
If every eigenvalue of a matrix A has the geometric multiplicity 1*, then A is called nonderogatory.*

Lemma 14 (Nonderogatory Matrix)
An $n \times n$ matrix A is nonderogatory if and only if its Frobenius normal form F consists of only one companion block.

This lemma is easily proved by Lemmas 8 and 9. Hence, we can determine the nonderogatoriness of a matrix by computing its Frobenius normal form.

On the other hand, the diagonalizability of a matrix, which is fundamental in linear algebra, is also determined by its Frobenius normal form.

Definition 15 (Diagonalizability)
If there exists a suitable regular matrix V for a matrix A such that $V^{-1}AV$ is diagonal, then A is called diagonalizable.

Lemma 16 (Diagonalizable Matrix)
An $n \times n$ matrix A is diagonalizable if and only if its minimal polynomial $\phi_A(x)$ is square-free.

The family of commutative matrices have the following property, which is applicable to the multiplication tables.

Lemma 17 (Commutativity and Common Eigenvector)
Let matrices A, B be commutative: $AB = BA$. And let $\boldsymbol{v}$ be an eigenvector of A with the eigenvalue λ, whose geometric multiplicity is 1. Then, this vector $\boldsymbol{v}$ is also an eigenvector of B.

Proof Since we have $A\boldsymbol{v} = \lambda\boldsymbol{v}$ and $AB = BA$, we obtain

$$A(B\boldsymbol{v}) = (AB)\boldsymbol{v} = (BA)\boldsymbol{v} = B(A\boldsymbol{v}) = B(\lambda\boldsymbol{v}) = \lambda(B\boldsymbol{v}).$$

Hence, $B\boldsymbol{v}$ also belongs to the eigenspace of A with the eigenvalue λ. Since λ has the geometric multiplicity 1, we have $B\boldsymbol{v} \in \mathrm{span}(\boldsymbol{v})$. Therefore, we obtain $B\boldsymbol{v} = \mu\boldsymbol{v}$ for a certain scalar μ. This means that $\boldsymbol{v}$ is an eigenvector of B having μ as the eigenvalue. ∎

3 Algorithms by Analysis of Multiplication Tables

Let $n \times n$ matrices $A_{x_1}, \ldots, A_{x_s}$ be the multiplication tables in Definition 2. We put $A := A_{x_k}$ for an arbitrary variable x_k.

First, we compute the Frobenius normal form F of A and a transformation matrix S such that $F = S^{-1}AS$. According to Lemmas 14 and 16, we determine the nonderogatoriness and diagonalizability of A. Then, we divide the problem into four cases, which correspond to the following four subsections.

3.1 Nonderogatory and Diagonalizable Case

In this case, F consists of only one companion block C (2), that is, $F = C$. Since the minimal polynomial $\phi_A(\lambda) = \varphi_C(\lambda) = \lambda^n - c_{n-1}\lambda^{n-1} - \cdots - c_1\lambda - c_0$ is square-free, the

n eigenvalues λ_j $(j = 1, \ldots, n)$ are simple and distinct. Then, Stetter's method (Theorem 4) can be directly applied to symbolic computation.

Algorithm 1 (Nonderogatory and Diagonalizable)
Initialize the list of solutions Sol $:= \{\ \}$, *and for* $j := 1$ *to* n, *do the following steps.*
1) $\boldsymbol{u}_j := \left[1, \lambda_j, \lambda_j^2, \ldots, \lambda_j^{n-1}\right]^T$.
2) $\boldsymbol{v}_j := S\boldsymbol{u}_j$.
3) *Normalize the first element of* $\boldsymbol{v}_j$ *to* 1; *(See* Remark 1*).*
4) *Let* $\boldsymbol{a}_{(i)1}^T$ *be the first row of* A_{x_i} $(i = 1, \ldots, s)$, *and compute a zero*

$$\boldsymbol{z}_j = \begin{bmatrix} z_{1j} \\ z_{2j} \\ \vdots \\ z_{sj} \end{bmatrix} := \begin{bmatrix} \boldsymbol{a}_{(1)1}^T \\ \boldsymbol{a}_{(2)1}^T \\ \vdots \\ \boldsymbol{a}_{(s)1}^T \end{bmatrix} \boldsymbol{v}_j.$$

5) Sol $:=$ Sol $\cup\{\boldsymbol{z}_j\}$.

Proof From Lemma 8, $\boldsymbol{u}_j$ is an eigenvector of $F = C$. Hence, $\boldsymbol{v}_j$ is an eigenvector of A from Lemma 10. Since λ_j has the geometric multiplicity 1, $\boldsymbol{v}_j$ is a common eigenvector of all the A_{x_i}'s from Lemmas 3 and 17.

Corresponding eigenvalues are given by $A_{x_i}\boldsymbol{v}_j = \mu_{ij}\boldsymbol{v}_j$. However, since the first element of $\boldsymbol{v}_j$ is normalized to 1, the first element of $\mu_{ij}\boldsymbol{v}_j$ is μ_{ij} itself. Hence, it is sufficient to compute only with the first row of A_{x_i}'s. ∎

Remark 1
The first row of S *becomes* $[1, 0, \ldots, 0]$ *in most cases because of the process of computing the Frobenius normal form. Then, the first element of* $\boldsymbol{v}_j$ *is already* 1, *and we do not need to apply step 3) in practice.*

If it happens to be 0, we have to select another non-zero element and utilize the corresponding row of A_{x_i}*'s. However, we have not found such an example at present.*

Example 1 (Example 1 in [6])

$$\begin{cases} p_1 = 3x^2y + 9x^2 + 2xy + 5x + y - 3 \\ p_2 = 2x^3y + 6x^3 - 2x^2 - xy - 3x - y + 3 \\ p_3 = x^3y + 3x^3 + x^2y + 2x^2 \end{cases}$$

According to the reference, we compute with *gradlex* order $(x > y)$, and we obtain the normal set basis $B = \{1, y, x\}$. Then, the multiplication tables are computed as follows:

$$A_x = \begin{bmatrix} & & 1 \\ -3 & 1 & -1 \\ 3 & -1 & \frac{3}{2} \end{bmatrix}, \qquad A_y = \begin{bmatrix} & 1 & \\ \frac{3}{2} & \frac{5}{2} & 4 \\ -3 & 1 & -1 \end{bmatrix}.$$

Computing the Frobenius normal form of A_x, we obtain

$$F = \begin{bmatrix} & 1 & \\ & & 1 \\ 0 & \frac{5}{2} & \frac{5}{2} \end{bmatrix}, \qquad S = \begin{bmatrix} 1 & & \\ 3 & \frac{3}{2} & -1 \\ & 1 & \end{bmatrix},$$

hence, A_x is nonderogatory. The minimal polynomial of A_x is $\phi(\lambda) = \lambda^3 - (5/2)\lambda^2 - (5/2)\lambda$, which is square-free, then A_x is diagonalizable.

Let λ_1, λ_2 be the roots of $\lambda^2 - (5/2)\lambda - 5/2$, and we get the eigenvectors of F with the eigenvalues $\lambda_1, \lambda_2, 0$ respectively:

$$\boldsymbol{u}_1 = \begin{bmatrix} 1 \\ \lambda_1 \\ \frac{5}{2}\lambda_1 + \frac{5}{2} \end{bmatrix}, \qquad \boldsymbol{u}_2 = \begin{bmatrix} 1 \\ \lambda_2 \\ \frac{5}{2}\lambda_2 + \frac{5}{2} \end{bmatrix}, \qquad \boldsymbol{u}_3 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}.$$

Then, the eigenvectors of A_x are given by $\boldsymbol{v}_j = S\boldsymbol{u}_j$:

$$\boldsymbol{v}_1 = \begin{bmatrix} 1 \\ -\lambda_1 + \frac{1}{2} \\ \lambda_1 \end{bmatrix}, \qquad \boldsymbol{v}_2 = \begin{bmatrix} 1 \\ -\lambda_2 + \frac{1}{2} \\ \lambda_2 \end{bmatrix}, \qquad \boldsymbol{v}_3 = \begin{bmatrix} 1 \\ 3 \\ 0 \end{bmatrix}.$$

Consequently, we obtain the 3 simple zeros:

$$\begin{bmatrix} \boldsymbol{a}_{(x)1}^T \\ \boldsymbol{a}_{(y)1}^T \end{bmatrix} \boldsymbol{v}_1 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ -\lambda_1 + \frac{1}{2} \\ \lambda_1 \end{bmatrix} = \begin{bmatrix} \lambda_1 \\ -\lambda_1 + \frac{1}{2} \end{bmatrix},$$

$$\begin{bmatrix} \boldsymbol{a}_{(x)1}^T \\ \boldsymbol{a}_{(y)1}^T \end{bmatrix} \boldsymbol{v}_2 = \begin{bmatrix} \lambda_2 \\ -\lambda_2 + \frac{1}{2} \end{bmatrix}, \qquad \begin{bmatrix} \boldsymbol{a}_{(x)1}^T \\ \boldsymbol{a}_{(y)1}^T \end{bmatrix} \boldsymbol{v}_3 = \begin{bmatrix} 0 \\ 3 \end{bmatrix}.$$

3.2 Nonderogatory and Nondiagonalizable Case

In this case, F consists of only one companion block C (2), that is, $F = C$. Let the minimal polynomial $\phi_A(\lambda) = \varphi_C(\lambda) = \lambda^n - c_{n-1}\lambda^{n-1} - \cdots - c_1\lambda - c_0$ have r $(r < n)$ roots. We let the algebraic multiplicity of each eigenvalue λ_j be p_j $(j = 1, \ldots, r)$.

Algorithm 2 (Nonderogatory and Nondiagonalizable)
Initialize the list of solutions $\mathrm{Sol} := \{\}$, *and the list of multiplicities* $\mathrm{Mul} := \{p_1, p_2, \ldots, p_r\}$.
For $j := 1$ *to* r, *do the following steps.*
1) $\boldsymbol{u}_j := \left[1, \lambda_j, \lambda_j^2, \ldots, \lambda_j^{n-1}\right]^T$.
2) $\boldsymbol{v}_j := S\boldsymbol{u}_j$.

3) *Normalize the first element of* $\boldsymbol{v}_j$ *to* 1; *(See* Remark 1*).*
4) *Let* $\boldsymbol{a}_{(i)1}^T$ *be the first row of* A_{x_i} $(i = 1, \ldots, s)$*, and compute a zero*

$$\boldsymbol{z}_j = \begin{bmatrix} z_{1j} \\ z_{2j} \\ \vdots \\ z_{sj} \end{bmatrix} := \begin{bmatrix} \boldsymbol{a}_{(1)1}^T \\ \boldsymbol{a}_{(2)1}^T \\ \vdots \\ \boldsymbol{a}_{(s)1}^T \end{bmatrix} \boldsymbol{v}_j.$$

5) Sol := Sol $\cup\{\boldsymbol{z}_j\}$.

Proof Since each eigenvalue has the geometric multiplicity 1, $\boldsymbol{v}_j$ is a common eigenvector similarly to Algorithm 1. The multiplicities of each zero $\boldsymbol{z}_j$ coincides with p_j from Theorem 4. ∎

Remark 2
We obtain the locations and the multiplicities of all the zeros by this algorithm. For more minute description of multiple zeros, see [22], which shows the formula for the simultaneous transformation of the A_{x_i}*'s into upper triangular block diagonal forms.*

Example 2 (Example 2 in [6])

$$\begin{cases} p_1 = x^2 + y^2 - 1 \\ p_2 = (3x + 4y)^2 + \frac{(-4x+3y)^2}{2} - 25 \end{cases}$$

According to the reference, we compute with *gradlex* order $(x > y)$, and we obtain the normal set basis $B = \{1, y, x, y^2\}$. Then, the multiplication tables A_x, A_y become 4×4 matrices. Computing the Frobenius normal form of A_x, we obtain

$$F = \begin{bmatrix} & 1 & & \\ & & 1 & \\ & & & 1 \\ -\frac{81}{625} & 0 & \frac{18}{25} & 0 \end{bmatrix}, \qquad S = \begin{bmatrix} 1 & & & \\ & \frac{19}{8} & & -\frac{625}{216} \\ & 1 & & \\ 1 & & -1 & \end{bmatrix},$$

hence, A_x is nonderogatory. The minimal polynomial of A_x is

$$\phi(\lambda) = \lambda^4 - \frac{18}{25}\lambda^2 + \frac{81}{625} = \left(\lambda - \frac{3}{5}\right)^2 \left(\lambda + \frac{3}{5}\right)^2,$$

which is not square-free, then A_x is nondiagonalizable.

The eigenvalues $\lambda_1 = 3/5$ and $\lambda_2 = -3/5$ respectively have the algebraic multiplicity 2 and the geometric multiplicity 1. Hence, both $x = 3/5$ and $x = -3/5$ constitute double zeros. Corresponding eigenvectors of F are

$$\boldsymbol{u}_1 = \begin{bmatrix} 1 \\ \frac{3}{5} \\ \frac{9}{25} \\ \frac{27}{125} \end{bmatrix}, \qquad \boldsymbol{u}_2 = \begin{bmatrix} 1 \\ -\frac{3}{5} \\ \frac{9}{25} \\ -\frac{27}{125} \end{bmatrix}.$$

Consequently, we obtain the 2 double zeros:

$$\begin{bmatrix} \boldsymbol{a}_{(x)1}^T \\ \boldsymbol{a}_{(y)1}^T \end{bmatrix} (S\boldsymbol{u}_1) = \begin{bmatrix} \frac{3}{5} \\ \frac{4}{5} \end{bmatrix}, \qquad \begin{bmatrix} \boldsymbol{a}_{(x)1}^T \\ \boldsymbol{a}_{(y)1}^T \end{bmatrix} (S\boldsymbol{u}_2) = \begin{bmatrix} -\frac{3}{5} \\ -\frac{4}{5} \end{bmatrix}.$$

3.3 Derogatory and Diagonalizable Case

We assume that the multiplication table A_{x_k} is derogatory and diagonalizable. In this case, we compute the Frobenius normal forms of other multiplication tables A_{x_i} ($i = 1, \ldots, s$; $i \neq k$). If there exists at least one nonderogatory A_{x_ℓ}, then we can let $A := A_{x_\ell}$ and apply Algorithm 1 or Algorithm 2 according to its diagonalizability.

Now we consider the case where all the multiplication tables A_{x_i} ($i = 1, \ldots, s$) are derogatory. If there exists at least one nondiagonalizable A_{x_ℓ} among them, then we have to apply the case §3.4.

Otherwise, if all the A_{x_i}'s are diagonalizable, the following theorem in linear algebra is applicable to the family $\{A_{x_i}\}$.

Theorem 18 (Commutative and Diagonalizable Matrices)
Let A, B be commutative matrices: $AB = BA$. Moreover, we assume that both A and B are diagonalizable. Then, there exists a set of common eigenvectors $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ of A and B such that both $V^{-1}AV$ and $V^{-1}BV$ are diagonal, where $V = [\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n]$.

To find such common eigenvectors for the family $\{A_{x_i}\}$, we put $A_w := \sum_{i=1}^{s} c_i A_i$ with randomly selected integers c_i. Then, A_w becomes nonderogatory for almost every s-tuple $(c_1, \ldots, c_s)$ [28]. Since $V^{-1}A_wV = V^{-1}\left(\sum c_iA_i\right)V = \sum c_i\left(V^{-1}A_iV\right)$, A_w is also diagonalizable, then we can apply Algorithm 1 to A_w.

From the viewpoint of a system of algebraic equations, this situation corresponds to the case where all the zeros are simple but some of them have the same x_i-coordinate in common. In such a case, we can make the system into general position by almost every linear coordinate transformation $w := c_1x_1 + \cdots + c_sx_s$. Now we summerize the above flow.

Algorithm 3 (Derogatory and Diagonalizable)

% Assumption: The A_{x_k} is derogatory and diagonalizable.

Compute all the Frobenius normal forms of the A_{x_i}'s and apply one of the following.

% Case (A): Some A_{x_ℓ} is nonderogatory.

Apply Algorithm 1 or 2 according to its diagonalizability.

% Case (B): All the A_{x_i}'s are derogatory and some A_{x_ℓ} is nondiagonalizable.

Apply the case §3.4.

% Case (C): All the A_{x_i}'s are derogatory and diagonalizable.

Put $A_w := \sum_{i=1}^{s} c_i A_i$ with random $(c_1, \ldots, c_s)$ so that A_w is nonderogatory.

Then, apply Algorithm 1 to A_w.

Remark 3

- *Since the selection of $(c_1, \ldots, c_s)$ is heuristic, this step is probablistic. Strictly speaking, we should consider applying deterministic methods [23][28] for finding a generic tuple.*
- *In case (A), it is sufficient to find at least one nonderogatory matrix A_{x_ℓ}. On the other hand, in case (C), it is necessary to confirm that all the A_{x_i}'s are diagonalizable.*
- *In order to characterize the matrix family $\{A_{x_i}\}$, we have to compute all the Frobenius normal forms. Instead, only to find a nonderogatory one, it might be practical to start on $\sum_{i=1}^{s} c_i A_i$ directly. It is a trade-off with the cost where the sparsity is destroyed.*

Example 3 (Cyclic 3rd Root)

$$\begin{cases} p_1 = x + y + z \\ p_2 = xy + yz + zx \\ p_3 = xyz - 1 \end{cases}$$

We compute with *gradlex* order $(x > y > z)$, and we obtain the normal set basis $B = \{1, z, y, z^2, yz, yz^2\}$. Then, the multiplication tables A_x, A_y, A_z becomes 6×6 matrices. The Frobenius normal form of each matrix consists of 2 companion blocks, with the associated polynomials $\varphi_1(\lambda) = \varphi_2(\lambda) = \lambda^3 - 1$. This means that all of A_x, A_y, A_z are derogatory and diagonalizable. (They have naturally the same structure because of the symmetry of variables x, y, z.)

Then, we try putting $A_w := A_x + 2A_y - A_z$ and computing its Frobenius normal form F and a transformation matrix S such that $A_w S = SF$. As a result, we obtain

$$F = \begin{bmatrix} & 1 & & & & \\ & & 1 & & & \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & 1 \\ -343 & 0 & 0 & -20 & 0 & 0 \end{bmatrix},$$

thus, A_w is nonderogatory as expected. The minimal polynomial of A_w is

$$\phi(\lambda) = \lambda^6 + 20\lambda^3 + 343 = \left(\lambda^2 + 5\lambda + 7\right)\left(\lambda^2 - \lambda + 7\right)\left(\lambda^2 - 4\lambda + 7\right),$$

which is square-free, then A_w is also diagonalizable.

Hence, we apply Algorithm 1 to A_w. We let the eigenvalues as follows:
$\lambda_{11}, \lambda_{12}$ are the roots of $\lambda^2 + 5\lambda + 7$,
$\lambda_{21}, \lambda_{22}$ are the roots of $\lambda^2 - \lambda + 7$,
$\lambda_{31}, \lambda_{32}$ are the roots of $\lambda^2 - 4\lambda + 7$.
We put the eigenvectors of F as $\boldsymbol{u}_{ij} := \left[1, \lambda_{ij}, \lambda_{ij}^2, \ldots, \lambda_{ij}^5\right]^T$, and reduce each element using the definition polynomials of λ_{ij} $(i = 1, 2, 3;\ j = 1, 2)$. Then, the eigenvectors of A_w are given by $\boldsymbol{v}_{ij} = \boldsymbol{S}\boldsymbol{u}_{ij}$. Using these 6 common eigenvectors, we obtain the 6 simple zeros:

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} -\lambda_{1j} - 3 \\ \lambda_{1j} + 2 \\ 1 \end{bmatrix}, \quad \begin{bmatrix} 1 \\ \frac{1}{3}\lambda_{2j} - \frac{2}{3} \\ -\frac{1}{3}\lambda_{2j} - \frac{1}{3} \end{bmatrix}, \quad \begin{bmatrix} \frac{1}{2}\lambda_{3j} - \frac{3}{2} \\ 1 \\ -\frac{1}{2}\lambda_{3j} + \frac{1}{2} \end{bmatrix} \qquad (j = 1, 2).$$

3.4 Derogatory and Nondiagonalizable Case

In this case, all of the A_{x_i}'s are derogatory, and some of them are nondiagonalizable. We cannot immediately distinguish a multiple zero from simples zeros with the same x_i-coordinate. Therefore, we have to handle the system depending on the case.

In some cases, it is still effective to make a linear combination with random $(c_1, \ldots, c_s)$. If we obtain a nonderogatory $A_w = \sum_{i=1}^{s} c_i A_i$, then we can apply Algorithm 1 or 2 to A_w. The following example belongs to such a case.

Example 4 (Example 3 in [6])

$$\begin{cases} p_1 = x^2 + y^2 - 1 \\ p_2 = x^3 + (2 + z)xy + y^3 - 1 \\ p_3 = z^2 - 2 \end{cases}$$

According to the reference, we compute with *gradlex* order $(x > y > z)$, and we obtain the normal set basis with 12 elements. Then, this system has 12 solutions and the multiplication tables A_x, A_y, A_z become 12×12 matrices.

The Frobenius normal form of A_x contains 2 companion blocks, and its minimal polynomial is

$$\phi_{A_x}(\lambda) = (\lambda^4 - 2\lambda^3 + \lambda^2 + 8\lambda + 8)\lambda(\lambda - 1)\left(\lambda^2 - 1/2\right)^2,$$

hence, A_x is derogatory and nondiagonalizable. The matrix A_y has the same structure as A_x. The Frobenius normal form of A_z contains 6 companion blocks, and its minimal polynomial is $\phi_{A_z}(\lambda) = \lambda^2 - 2$, hence, A_z is derogatory but diagonalizable. However, the family $\{A_x, A_y, A_z\}$ are not diagonalizable.

Then, we try putting $A_w := A_x - A_y + A_z$ and computing its Frobenius normal form. Consequently, we find it nonderogatory and its minimal polynomial to be

$$\phi_{A_w}(\lambda) = \left(\lambda^4 + 10\lambda^2 + 32\lambda + 49\right)\left(\lambda^2 + 2\lambda - 1\right)\left(\lambda^2 - 2\lambda - 1\right)\left(\lambda^2 - 2\right)^2.$$

We let the eigenvalues as follows:

$\lambda_{11}, \ldots, \lambda_{14}$ are the roots of $\lambda^4 + 10\lambda^2 + 32\lambda + 49$,

$\lambda_{21}, \lambda_{22}$ are the roots of $\lambda^2 + 2\lambda - 1$,

$\lambda_{31}, \lambda_{32}$ are the roots of $\lambda^2 - 2\lambda - 1$,

$\lambda_{41}, \lambda_{42}$ are the roots of $\lambda^2 - 2$.

The eigenvalues $\lambda_{41}, \lambda_{42}$ have the algebraic multiplicity 2 and the geometric multiplicity 1. Hence, the matrix A_w is nondiagonalizable, and we apply Algorithm 2 to it. Constructing 10 common eigenvectors, we obtain the following zeros:

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \underset{(j=1,\ldots,4)}{\begin{bmatrix} -\frac{1}{52}\lambda_{1j}^3 - \frac{1}{26}\lambda_{1j}^2 + \frac{25}{52}\lambda_{1j} - \frac{2}{13} \\ -\frac{3}{52}\lambda_{1j}^3 - \frac{3}{26}\lambda_{1j}^2 - \frac{29}{52}\lambda_{1j} - \frac{19}{13} \\ -\frac{1}{26}\lambda_{1j}^3 - \frac{1}{13}\lambda_{1j}^2 - \frac{1}{26}\lambda_{1j} - \frac{17}{13} \end{bmatrix}}, \underset{(j=1,2)}{\begin{bmatrix} 0 \\ 1 \\ \lambda_{2j}+1 \end{bmatrix}}, \underset{(j=1,2)}{\begin{bmatrix} 1 \\ 0 \\ \lambda_{3j}-1 \end{bmatrix}}, \underset{(j=1,2)}{\begin{bmatrix} -\frac{1}{2}\lambda_{4j} \\ -\frac{1}{2}\lambda_{4j} \\ \lambda_{4j} \end{bmatrix}}.$$

The first 8 zeros are simple, and the last 2 are double. In [6], the derogatoriness of A_x has caused confusion and misled the 4 simple zeros with $x = 0, 1$ into 2 double zeros.

In other cases, we may fail to find a nonderogatory A_w by a linear combination $\sum_{i=1}^{s} c_i A_i$. Such situation indicates the existence of multiple zeros, but it is difficult to find common eigenvectors without heuristics. Therefore, we try to compute the radical $\sqrt{I}$ of the ideal I, because the locations of their zeros are coincident. The multiplicities can be counted by comparing the characteristic polynomial in R/I and the minimal polynomial in $R/\sqrt{I}$.

Note that all the Frobenius normal forms of the A_{x_i} $(i = 1, \ldots, s)$ have been already computed, that is, we have obtained all the minimal polynomials of the A_{x_i}'s at this point. Then, the following facts are applicable.

Lemma 19 (Minimal Univariate Polynomial in I)
Let A_{x_i} be the multiplication table in $\mathbf{Q}[x_1, \ldots, x_s]/I$, where I is zero-dimensional. And let $\phi_i(\lambda)$ be the minimal polynomial of the matrix A_{x_i}. Then, $\phi_i(x_i)$ is the unique monic univariate polynomial of minimal degree in $I \cap \mathbf{Q}[x_i]$.

Theorem 20 (Theorem 8.22 of [2])
Let $h_i(x_i)$ be the square-free part of $\phi_i(x_i)$ in the above lemma. Then, we have $\sqrt{I} = (I, h_1(x_1), \ldots, h_s(x_s))$.

We have already computed the Gröbner basis G of the ideal I. Hence, we compute again with a new (smaller) system $\{G, h_1, \ldots, h_s\}$. Since all the zeros of $\sqrt{I}$ are simple, the family of new multiplication tables is always diagonalizable. Therefore, we can find a nonderogatory matrix (by a linear combination, if necessarily).

Example 5 (Example 2 in [15])
For the polynomials $f_1 = x^2 - xy - y^2 + 1$ and $f_2 = xy + 3y^2 + 1$, we define $p_1 := f_1^2 - f_2^2$ and $p_2 := 2f_1^2 + 3f_2^2$. Here, We consider the zeros of the ideal $I = (p_1, p_2)$.

We compute with *gradlex* order $(x > y)$, and we obtain the normal set basis with 16 elements. Then, this system has 16 solutions and the multiplication tables A_x, A_y become 16×16 matrices.

The Frobenius normal form of A_x contains 2 companion blocks (12×12 and 4×4), and its minimal polynomial is $\phi_{A_x}(\lambda) = \left(\lambda^4 + (28/11)\lambda^2 + 16/11\right)^3$, hence, A_x is derogatory and nondiagonalizable. Similarly, the Frobenius normal form of A_y contains 2 companion blocks (12×12 and 4×4), and its minimal polynomial is $\phi_{A_y}(\lambda) = \left(\lambda^4 + (8/11)\lambda^2 + 1/11\right)^3$. In this case, we cannot find a nonderogatory matrix by a linear combination $c_1A_x + c_2A_y$. For example, $A_w := 3A_x + 7A_y$ has the same structure as A_x and A_y.

Now we compute the radical of I. Let $q_x := x^4 + (28/11)x^2 + 16/11$, $q_y := y^4 + (8/11)y^2 + 1/11$, and we consider the system $\{G, q_x, q_y\}$, where G is the Gröbner basis of $I = (p_1, p_2)$. Eventually, the new matrix $\bar{A}_x$ is nonderogatory and its minimal polynomial is $\phi_{\bar{A}_x}(\lambda) = \lambda^4 + (28/11)\lambda^2 + 16/11$. Consequently, we obtain the 4 simple zeros $(i = 1, \ldots, 4)$ of $\sqrt{I}$:

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \lambda_i \\ -\frac{11}{8}\lambda_i^3 - 2\lambda_i \end{bmatrix}, \quad \text{where } \phi_{\bar{A}_x}(\lambda_i) = 0.$$

In this example, the ideal I is primary, therefore, each solution has the same multiplicity $16/4 = 4$ by Theorem 3.3 in [15]. In fact, we have $\varphi_{A_x}(\lambda) = \{\phi_{\bar{A}_x}(\lambda)\}^4$.

4 Implementation and Timing Data

We have implemented the above-mentioned algorithms on the computer algebra system Reduce3.6. Gröbner bases are computed using the library package in Reduce, and Frobenius normal forms are computed using the program written by the authors [21]. Using IBM ThinkPad 535 (Pentium 120MHz processor) with 32MB memory, we solved several problems. For comparison, we applied aslo the FGLM algorithm [10] using Reduce library function *GLEXCONVERT*.

The detection of derogatory cases is not fully implemented yet. Random integers $(c_1, \ldots, c_s)$ are heuristically selected, and the derogatoriness is manually determined after some trial and error.

In addition to the examples shown in the previous section, the following examples are computed. The timing data is shown in the Table 1.

Example 6 (Katsura 5)
This system has 32 simple zeros. We compute its Gröbner basis with *revgradlex* order ($u_0 > u_1 > \cdots > u_5$). The result is rather dense.

Example 7 (Katsura 6)
This system has 64 simple zeros. We compute its Gröbner basis with *revgradlex* order ($u_0 > u_1 > \cdots > u_6$). The result is very dense.

Example 8 (Cyclic 5th Roots from [10])
This system has 70 simple zeros. We compute its Gröbner basis with *revgradlex* order ($x_1 > x_2 > \cdots > x_5$). The matrix for each variable is expected to have the same structure analogously to Example 3.3. Therefore, after confirming that matrix A_{x_1} is derogatory and diagonalizable, we omit the computation of the Frobenius normal forms of $A_{x_2}, \ldots, A_{x_5}$. Then, we put $A_w := A_{x_1} - 3A_{x_2} + 5A_{x_3} - 7A_{x_4} + 11A_{x_5}$ and compute its Frobenius normal form, to find it nonderogatory.

Example 9 ("A harder problem" in [7])
This system has 49 zeros (21 double and 7 simple). We compute its Gröbner basis with *revgradlex* order ($y > x$). The matrix A_y is derogatory but A_x is nonderogatory, hence, it is a good-natured problem.

Example 10 (Caprasse's System from [10])
This system has 56 zeros (8 quadruple and 24 simple). Most zeros are mutually related through the same coordinates in particular variables.

We compute its Gröbner basis with *revgradlex* order ($t > z > y > x$). We could not find a nonderogatory matrix by a linear combination, for example, $A_w := A_t + 3A_z - 5A_y - 7A_x$. Computing the radical, and putting $\bar{A}_w := \bar{A}_t + 3\bar{A}_z - 5\bar{A}_y - 7\bar{A}_x$, finally we found a nonderogatory matrix. The multiplicities are determined by comparing the characteristic polynomial φ_w of A_w (in R/I) and the minimal polynomial $\bar{\phi}_w = \bar{\varphi}_w$ of $\bar{A}_w$ (in $R/\sqrt{I}$):

$$\varphi_w = \varphi_1^4 \varphi_2^4 \varphi_3^4 \varphi_4^4 \times \tilde{\varphi}, \qquad \bar{\phi}_w = \bar{\varphi}_w = \varphi_1 \varphi_2 \varphi_3 \varphi_4 \times \tilde{\varphi},$$

where $\deg \varphi_i = 2$ $(i = 1, \ldots, 4)$ and $\tilde{\varphi}$ is square-free.

5 Discussion

5.1 Comparison with other methods

The output of the proposed method is identical to the lexicographical Gröbner basis in general position. For such a purpose, *change of ordering* methods have been studied. In particular, the FGLM algorithm is very efficient, and the Reduce library function *GLEXCONVERT* solved all of the previous examples faster than our program, except for "Katsura 6", as shown in the Table 1.

On the other hand, *the rational univariate representation (RUR)* method is proposed to obtain a compact representation of the zeros, and its improvement is being studied [23][24]. From the viewpoint of practical efficiency, the *RUR* method is most recommended.

5.2 Comparison with Stetter's numerical approach

We have shown the exact computation algorithm for solving a system of algebraic equations by matrix eigenproblems, which is the symbolic version of Stetter's method. Although efficient and reliable numerical library programs are now available, the precision problem becomes more serious for larger systems. In particular, when the system has multiple zeros or spurious multiple zeros (simple zeros with the same coordinate in a certain variable), their detection as a cluster must be rather heuristic [7].

On the other hand, our symbolic approach gives a good insight into multiple eigenvalues. For the nonderogatory case, the solutions can be symbolically determined together with their multiplicities. Moreover, it leads to a constructive description of multiple zeros [22], which is in contrast to the formulation by Möller and Stetter [19][20][26].

5.3 Complexity

Here we roughly estimate the cost of the matrix eigenproblem method. Let $n = \dim_{\mathbf{Q}} (\mathbf{Q}[x_1, \ldots, x_s]/I)$. After computing a Gröbner basis for I, we perform the following steps.

(1) Computation of the multiplication tables
The cost is estimated at $O(sn^3)$ arithmetic operations over $\mathbf{Q}$ [10][23][24].

(2) Computation of the Frobenius normal forms
When the size of a matrix is $n \times n$, Danilevskii's method computes its characteristic polynomial with $O(n^3)$ arithmetic operations [9]. Our implementation based on [13] is considered to have the same complexity. Since we have to compute $(s+1)$ normal forms at most, the total cost of this step is $O(sn^3)$.

(3) Construction of zeros using common eigenvectors
The computation of an eigenvector consists of multiplying an $n \times n$ matrix by an n-vector, whose cost is $O(n^2)$. The construction of a zero consists of multiplying an $s \times n$ matrix by an n-vector, whose cost is $O(sn)$. Since the maximal number of zeros is n, the total cost of this step is $O(n^3 + sn^2)$.

Consequently, the total number of arithmetic operations over $\mathbf{Q}$ through these steps is estimated at $O(sn^3)$. However, in the step (2), the elements of the matrices often grow into huge rational numbers, thus we need an estimation based on machine operations considering coefficient growth. Nevertheless, such one for Frobenius normal forms is not known, and further analysis is very difficult at present.

5.4 Improvement of efficiency

The Table 1 shows that the step of Frobenius normal forms computation is dominant in our present implementation, even though it did not cause the memory shortage in these examples.

The complexity of Frobenius normal form $O(n^3)$ is the same order as that of Gaussian elimination, and the total cost $O(sn^3)$ is the same as that of the FGLM algorithm [10]. Therefore, the matrix eigenproblem method could compare favorably with FGLM. However, the existing programs for Frobenius normal forms [5][12] are not efficient enough, because the intermediate swells are explosive. Our program seems rather faster than they, but its improvement is needed. To avoid the coefficient growth, modular methods are generally promising, whose application should be considered in the future study.

5.5 Concluding Remarks

Computing the Frobenius normal forms of multiplication tables we divide the problem into four cases:

(1) nonderogatory and diagonalizable case,

(2) nonderogatory and nondiagonalizable case,

(3) derogatory and diagonalizable case,

(4) derogatory and nondiagonalizable case.

For the nonderogatory cases (1)(2), the solutions can be symbolically determined including multiple zeros.

If the family of matrices is diagonalizable in the case (3), there always exist nonderogatory matrices among linear combinations $A_w := \sum_{i=1}^{s} c_i A_i$ with randomly chosen integers c_i. Then, A_w becomes nonderogatory for almost every s-tuple $(c_1, \ldots, c_s)$. Actually, it might be practical to start on $\sum_{i=1}^{s} c_i A_i$ without computing each Frobenius normal form of A_i.

Only for the case (4), we need minute treatment depending on each problem. Theoretically, on the assumption of exact computation, the locations and the multiplicities of zeros can be algorithmically determined through the radical of the ideal. However, when it is hard to comput the radical of a large-sized system directly [23][24], we have to develop an algorithm for simultaneously decomposing the ideal in the context of matrix eigenproblems. This is still an open problem.

Acknowledgements

We are grateful to one of the anonymous referees for many valuable and helpful comments.

References

[1] Auzinger, W. and Stetter, H. J.: An Elimination Algorithm for the Computation of All Zeros of a System of Multivariate Polynomial Equations, *Numerical Mathematics Singapore 1988* (Agarwal, R. P., Chow, Y. M., and Wilson, S. J., eds.), *International Series of Numerical Mathematics*, **86**, Birkhäuser, Basel, 1988, 11–30.

[2] Becker, T. and Weispfenning, V.: *Gröbner Bases : A Computational Approach to Commutative Algebra*, Springer-Verlag, New York, 1993.

[3] Buchberger, B.: *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*, PhD thesis, Universität Innsbruck, 1965.

[4] Buchberger, B.: Ein Algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems, *Aequationes Mathematicae*, **4**(3), 1970, 374–383.

[5] Char, B. W., et al.: *Maple V Library Reference Manual*, Springer, N.Y., 1991.

[6] Corless, R. M.: Editor's Corner : Gröbner Bases and Matrix Eigenproblems, *ACM SIGSAM Bull.*, **30**(4), 1996, 26–32.

[7] Corless, R. M., Gianni, P., and Trager, B. M.: A Reordered Schur Factorization Method for Zero-dimensional Polynomial Systems with Multiple Roots, *ISSAC '97* (Küchlin, W. W., ed.), ACM, New York, 1997, 133–140.

[8] Danilevskii, A. M.: On the numerical solution of the secular equation, *Mat.Sb.*, **2**(1), 1937, 169–172. (in Russian).

[9] Faddeev, D. K. and Faddeeva, V. N.: *Computational Methods of Linear Algebra*, W.H.Freeman, San Francisco, 1963.

[10] Faugère, J. C., Gianni, P., Lazard, D., and Mora, T.: Efficient Computation of Zero-Dimensional Gröbner Basis by Change of Ordering, *J.Symb.Comput.*, **16**(4), 1993, 329–344.

[11] Gantmacher, F. R.: *The Theory of Matrices (2nd ed.)*, **1**, Chelsea, New York, 1959.

[12] Hearn, A. C.: *Reduce User's Manual (Ver. 3.6)*, RAND Corp., Santa Monica, 1995.

[13] Kan, T. and Iri, M.: *Jordan Normal Form*, Univ. of Tokyo Press, Tokyo, 1982. (in Japanese).

[14] Kobayashi, H., Fujise, T., and Furukawa, A.: Solving Systems of Algebraic Equations by a General Elimination Method, *J.Symb.Comput.*, **5**(3), 1988, 303–320.

[15] Kobayashi, H., Moritsugu, S., and Hogan, R. W.: Solving Systems of Algebraic Equations, *ISSAC '88* (Gianni, P., ed.), *Lect. Notes in Comp. Sci.*, **358**, Springer-Verlag, Berlin, 1989, 139–149.

[16] Lazard, D.: Algèbre linéaire sur $K[x_1, x_2, \ldots, x_n]$ et élimination, *Bull.Soc.Math.France*, **105**(2), 1977, 165–190.

[17] Lazard, D.: Résolution des systèmes d'équations algébriques, *Theor.Comp.Sci.*, **15**, 1981, 77–110.

[18] Marinari, M. G., Möller, H. M., and Mora, T.: Göbner Bases of Ideals Given by Dual Bases, *ISSAC '91* (Watt, S. M., ed.), ACM, New York, 1991, 55–63.

[19] Möller, H. M.: Systems of Algebraic Equations Solved by Means of Endomorphisms, *AAECC 10* (Cohen, G., Mora, T., and Moreno, O., eds.), *Lect. Notes in Comp. Sci.*, **673**, Springer-Verlag, Berlin, 1993, 43–56.

[20] Möller, H. M. and Stetter, H. J.: Multivariate Polynomial Equations with Multiple Zeros Solved by Matrix Eigenproblems, *Numer.Math.*, **70**(3), 1995, 311–329.

[21] Moritsugu, S. and Kuriyama, K.: Exact Computation of Jordan Normal Forms of Matrices by Computer Algebra, *Trans.Japan Soc.Indust.Appl.Math.*, **2**(1), 1992, 91–103. (in Japanese).

[22] Moritsugu, S. and Kuriyama, K.: On Multiple Zeros of Systems of Algebraic Equations, *ISSAC '99* (Dooley, S., ed.), ACM, N.Y., 1999, 23–30.

[23] Noro, M. and Yokoyama, K.: A Modular Method to Compute the Rational Univariate Representation of Zero-dimensional Ideals, *J.Symb.Comput.*, **28**(1&2), 1999, 243–263.

[24] Rouillier, F.: *Algorithmes efficaces pour l'étude des zéros réels des systèmes polynomiaux*, PhD thesis, Université de Rennes I, 1996.

[25] Stetter, H. J.: Multivariate Polynomial Equations as Matrix Eigenproblems, *Contributions in Numerical Mathematics* (Agarwal, R. P., ed.), *World Scientific Series in Applicable Analysis*, **2**, World Scientific, Singapore, 1993, 355–371.

[26] Stetter, H. J.: Matrix Eigenproblem are at the Heart of Polynomial System Solving, *ACM SIGSAM Bull.*, **30**(4), 1996, 22–25.

[27] Takeshima, T. and Yokoyama, K.: A Solution of Systems of Algebraic Equations - Application of Eigenvectors of Linear Maps on Residue Class Rings, *Comm.Symb.Algeb.Manip.*, **6**(4), 1990, 27–36. (in Japanese).

[28] Yokoyama, K., Noro, M., and Takeshima, T.: Solutions of Systems of Algebraic Equations and Linear Maps on Residue Class Rings, *J.Symb.Comput.*, **14**(4), 1992, 399–417.

Table 1: CPU-Time(msec) for the computation of some examples

(#sol)	Mult.Table	Frobenius N.Form		Solutions	Total	FGLM
Ex 3.1 (3)	550	170	(A_x)	220	940	110
Ex 3.2 (4)	720	390	(A_x)	220	1,330	50
Ex 3.3 (6)	1,440	601	(A_x)			
		610	(A_y)			
		550	(A_z)			
		1,138	(A_w)	610	4,949	170
Ex 3.4 (12)	5,271	6,750	(A_x)			
		6,490	(A_y)			
		3,020	(A_z)			
		7,190	(A_w)	1,320	30,041	1,870
Ex 3.4 (16)	7,750	16,320	(A_x)			
		18,670	(A_y)			
		17,140	(A_w)	(unable)	(59,880)	1,090
$\sqrt{I}$ (4)	720	319	$(\bar{A}_x)$	170	1,209	170
Ex 4 (32)	750,479	460,330	(A_{u_0})	19,070	1,229,879	462,911
Ex 4 (64)	11,005,850	53,843,230	(A_{u_0})	2,741,550	67,590,630	69,219,200
Ex 4 (70)	512,030	2,211,201	(A_{x_1})			
		1,673,650	(A_w)	111,560	4,508,441	181,910
Ex 4 (49)	301,379	815,280	(A_y)			
		1,295,120	(A_x)	49,820	2,461,599	597,200
Ex 4 (56)	353,939	828,800	(A_t)			
		827,880	(A_z)			
		674,671	(A_y)			
		1,072,310	(A_y)			
		1,328,880	(A_w)	(unable)	(5,086,480)	358,731
$\sqrt{I}$ (32)	53,000	93,310	$(\bar{A}_t)$			
		139,440	$(\bar{A}_z)$			
		92,110	$(\bar{A}_y)$			
		138,960	$(\bar{A}_x)$			
		158,239	$(\bar{A}_w)$	21,970	697,029	76,679

Mult.Table : Gröbner basis + Construction of multiplication tables
Frobenius N.Form : Frobenius normal form computation of a matrix
Solutions : Construction of solutions by common eigenvectors
FGLM : Gröbner basis + GLEXCONVERT