Far East Journal of Mathematical Sciences (FJMS)

http://www.pphmj.com
http://dx.doi.org/10.17654/MS101040855
Volume 101, Number 4, 2017, Pages 855-872 **ISSN: 0972-0871**

GREATEST COMMON DIVISORS OF EUCLIDEAN DOMAIN MATRICES

Nur Erawaty, Mawardi Bahri, Loecky Haryanto and Amir Kamal Amir

Program Study of Mathematics
Department of Mathematics
Faculty of Mathematics and Natural Sciences
Hasanuddin University
Perintis Kemerdekaan Street, Makassar
Post Code 90245, Indonesia

Abstract

One of the Euclidean domains is the ring of polynomials over reals. The notion of a greatest common divisor of two matrices with polynomial entries is well-defined. In this paper, the same notion is generalized to two matrices with entries from a Euclidean domain. In this generalization, the common divisors for matrices are defined as either a common left or right divisor depending on whether the two matrices have the same number of rows or have the same number of columns. In determining a greatest common divisor of two matrices with entries from a Euclidean domain, the left (or right) structure matrix is analyzed using the Smith form.

1. Introduction

Divisibility is an important concept in algebra and number theory. In the

Received: August 13, 2016; Revised: September 21, 2016; Accepted: September 22, 2016
2010 Mathematics Subject Classification: 13P25, 15A30.
Keywords and phrases: Smith form, Euclidean domain, structure matrix, greatest common divisors.

ring of integers, the concept is well known. The Euclidean domains have the divisibility property.

The divisibility of integers states: given two integers (or two polynomials) a and b, $a \neq 0$, b is said to be *divisible* by a if there is an integer (or a polynomial) c such that $b = ac = ca$ (because the commutativity on integer and polynomial multiplication), written $a \mid b$. The greatest common divisor (or known as gcd) of a and b is the greatest integer d such that $d \mid a$ and $d \mid b$. If there is a common divisor c of a and b, then c/d. We write $\gcd(a, b) = d$.

Unlike the ring of integers or polynomials, the ring of matrices does not have commutative property for multiplication, i.e., $AB \neq BA$ (in general). Let three matrices A, B, C be form the equation $A = BC$. In general, $A \neq CB$. In the equation, B and C are called *left* and *right divisors* of A, respectively.

The concept of the greatest common right divisor of polynomial matrices has been presented by Bitmead [12]. The methods involve recently studied generalized Sylvester and generalized Bezoutian resultant matrices, which require no polynomial operations. In [15], Prugsapitak construct a complete residue system in the ring of 2×2 matrices over a Euclidean domain and use it to provide a division algorithm for matrices in order to obtain a greatest common divisor of two matrices over a certain Euclidean domain. An Euclidean algorithm for integer matrices provided by Thomsen in [10]. The inspiration was from Knuth’s paper that considers the greatest common right divisor of integer matrices. From his remark, they inspired to look for a bridge between the “mathematician’s answers” and the “computer scientist’s answer”.

Some examples of Euclidean domains are the ring of integers, polynomials, proper rational functions (Vardulakis [3]), proper and stable rational functions (Vidyasagar [8]). When the entries of a matrix are from a

Euclidean domain, the matrix is called an *Euclidean domain* (*ED*-) *matrix*. There is a problem in determining a greatest common divisor of two such matrices. An ED-matrix T with rank r is equivalent to a diagonal matrix S_T of Smith form. In the Smith's form, matrix T can be factorized as a product of ED-matrices. The main purpose of this paper is to determine the greatest common left (or right) divisor of these factor matrices.

Canonical Smith form for a polynomial matrix can be found in Gantmacher [4], the concept of structure matrices of T that properly divides T is contained in the work of Pernebo [6]. For the concepts of left (or right) divisor, greatest left divisor, see Solak [7], Barnett [14] and references therein.

The resulting greatest common divisors of ED-matrices allow us to determine the solutions of matrix Diophantine equations. This is an application of the greatest common divisors of ED-matrices.

2. Prerequisites

In order to obtain the greatest common divisor of an ED-matrix, the left matrix structure that divides the ED-matrix, is needed. This left matrix structure is obtained from the Smith form.

2.1. Euclidean domain matrices

Definition 1. A Euclidean domain E is an integral domain which satisfies the following condition: there is a map $\partial : E \to \mathbb{N}$ ($\mathbb{N}$ non-negative integers) such that for every $a \in E,\ a \neq 0,\ \partial(a) \in N$ and

(i) For $a, b \in E,$ such that $ab \neq 0,\ \partial(ab) \geq \partial(a).$

(ii) For every $a, b \in E,\ \ b \neq 0,$ there exist two elements $q, r \in E$ such that $a = bq + r$ and either $r = 0$ or $\partial(r) < \partial(b)$ (Fraleigh [5]).

The notations and symbols from the previous statements are borrowed in the following theorem.

Definition 2. Given two elements $a, b \neq 0$ in E, we say a is *divisible* by b and $\partial(a) \geq \partial(b)$. Note that, if a is divisible by b, then the 'quotient' q is in E and the division is 'exact' if $r = 0$.

Definition 3. An ED-matrix is a matrix with entries in Euclidean domain. $E^{m \times n}$ symbolized as the set of ED-matrices of size $m \times n$.

Definition 4. Let $T \in E^{p \times m}$. Then the zeros of T are defined as the zeros of entries in E (Vardulakis [3]).

Definition 5. An ED-matrix $T \in E^{p \times p}$ is called *unimodular*, if there exists a matrix $\hat{T} \in E^{p \times p}$ such that $T\hat{T} = \hat{T}T = I_p$, equivalently, if $|T| = c,\ c \neq 0,\ c$ is a unit in E (Vardulakis [3]).

Definition 6. The degree of an ED-matrix $T \in E^{p \times m}$ is denoted by deg T and is defined as the maximum degree of all its maximum order (non-zero) minors (Vardulakis [3]).

2.2. Smith form

Every matrix in Euclidean domain is equivalent to a diagonal matrix called the *Smith form*. Use elementary row/column operations on ED-matrices that are defined by interchange of any two rows/columns, multiplication of row or column by a unit in E, or addition to row/column a multiple of any non-zero element of E of any other row/column (Cameron [13] and Howard [17]).

We describe a sequence of elementary row and column operations over reals, which when applied to a matrix A with $a_{11} \neq 0$ either yields a matrix C of the form

$$C = \begin{pmatrix} f_1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & C^* & \\ 0 & & & \end{pmatrix},$$

where f_1 is a monic and divides every element of C^*, or else yields a matrix B in which $b_{11} \neq 0$ and

$$\deg b_{11} < \deg a_{11}.$$

Assuming this, we start with our non-zero matrix A. By performing suitable row and column interchanges, we can assume that $a_{11} \neq 0$. Now repeatedly perform the algorithm mentioned above. Eventually, we must reach a matrix of type C, otherwise, we would produce an infinite strictly decreasing sequence of non-negative integers by virtue of inequalities of $\deg b_{11} < \deg a_{11}$. On reaching a matrix of type C, we stop if $C^* = 0$. Otherwise, we perform the above argument on C^* and so on, leaving a trail of diagonal elements as we go.

Two points must be made:

(1) Any elementary row or column operation on C^* corresponds to an elementary operation on C, which does not affect the first row or column of C.

(2) Any elementary operation on C^* gives a new C^* whose new entries are linear combinations over reals of the old ones; consequently, these new entries will still be divisible by f_1.

Hence, in due course, we will reach a matrix D which is in Smith canonical form.

We now present the details of the sequence of elementary operations mentioned above.

Case 1. There exist a_{1j} in row 1 with a_{11} not dividing a_{1j}. Then, by Euclid's division theorem,

$$a_{1j} = a_{11}q + b,$$

where $b \neq 0$ and $\deg b < \deg a_{11}$. Subtract q times column 1 from column j

and then interchange columns 1 and j. This yields a matrix of type B mentioned above.

Case 2. There exists a_{i1} in column 1 with a_{11} not dividing a_{i1}. Proceed as in Case 1, operating on rows rather than on columns, again reaching a matrix of type C.

Case 3. Here a_{11} divides every element in the first row and first column. Then, by subtracting suitable multiples of column 1 from the other columns, we can replace all the entries in the first row other than a_{11} by 0. Similarly, for the first column. We then have a matrix of the form

$$E = \begin{pmatrix} e_{11} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & E^* & \\ 0 & & & \end{pmatrix}.$$

If e divides every element of E^*, then we obtain a matrix of type C. Otherwise, there exists e_{ij} not divisible by e_{11}. We then add row i to row 1, thereby reaching Case 1 (Howard [17]).

Theorem 7. *Each ED-matrix $T \in E^{p \times m}$ of rank $T = r$, is equivalent to a diagonal matrix canonical form Smith S_T :*

$$S_T = \begin{bmatrix} f_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & f_2 & \cdots & 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & f_r & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{bmatrix},$$

where each f_i are monic and f_i divides f_{i+1} for $i = 1, 2, ..., r-1$ (*Erawaty* [9]).

Definition 8. Let $T \in E^{p \times m}$ with rank $T = r$. If the Smith canonical form for $r = p$ takes the form

$$S_T = \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 & 0 \end{bmatrix} = [I_p \quad 0_{p, m-p}],$$

then T is called *right unimodular*. And, if for $r = m$,

$$S_T = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 \\ 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \end{bmatrix} = \begin{bmatrix} I_m \\ 0_{p-m, m} \end{bmatrix},$$

then T is called *left unimodular* (Vardulakis [3]).

Theorem 9. *If T is multiplication of a finite number of elementary matrices, then T is unimodular* (*Howard* [17]).

3. Results and Discussion

3.1. Structure matrices

Greatest common divisor of two matrices with polynomial entries is well-defined (Vardulakis [2]). In this paper, the same notion is generalized to two matrices with entries from any Euclidean domain. We have now an important factorization of ED-matrix.

Theorem 10. *Each ED-matrix $T \in E^{p \times m}$ of rank $T = r$ can be factorized* (*in a non-unique way*) *as*

$$T = T_L' T_1$$

or as

$$T = \hat{T}_1 T'_R,$$

where $T_1 \in E^{r\times m}$ *is right unimodular and* $\hat{T}_1 \in E^{p\times r}$ *left unimodular*.

Proof. Let $T \in E^{p\times m}$ and S_T Smith form of T, so there are unimodular matrices $T_L \in E^{p\times p}$, $T_R \in E^{m\times m}$ such that

$$S_T = T_L T T_R,$$

$$T = T_L^{-1} S_T T_R^{-1}.$$

We partition T_R^{-1} as

$$T_R^{-1} = \begin{bmatrix} T_1 \\ T_2 \end{bmatrix},$$

where $T_1 \in E^{r\times m}$, $T_2 \in E^{(m-r)\times m}$ are right unimodular. Then

$$\begin{aligned} T &= T_L^{-1} S_T T_R^{-1} \\ &= T_L^{-1} \begin{bmatrix} D \\ 0_{p-r,\, r} \end{bmatrix} [I_r \quad 0_{r,\, m-r}] \begin{bmatrix} T_1 \\ T_2 \end{bmatrix} \\ &= T_L^{-1} \begin{bmatrix} D \\ 0_{p-r,\, r} \end{bmatrix} T_1 \\ &= T'_L T_1 \end{aligned}$$

with

$$T'_L = T_L^{-1} \begin{bmatrix} D \\ 0_{p-r,\, r} \end{bmatrix} \in E^{p\times r}.$$

Similarly, for T'_R.

Definition 11. T'_L is called the *left structure matrix* of T and T'_R is called the *right structure matrix* of T.

3.2. Common divisors of Euclidean domain matrices

Given three matrices A, B, C that satisfy $A = BC$, we say B to be a *left divisor* of A.

Definition 12. Let E be a Euclidean domain and suppose given $T_1 \in E^{p\times l}$, $T_2 \in E^{p\times t}$. Then T is greatest common left divisor of T_1 and T_2 if $T_1 = TB$ and $T_2 = TC$ for any $B \in E^{p\times l}$, $C \in E^{p\times t}$ and any other greatest common left divisor is a multiple of T.

Theorem 13. *Suppose given $T_1 \in E^{p\times l}$, $T_2 \in E^{p\times t}$ with $l + t = m \geq p = rank[T_1, T_2]$, and $T_L' \in E^{p\times p}$ is structure matrix of $T = [T_1, T_2] \in E^{p\times m}$. Then T_L' is a greatest common left divisor of T_1 and T_2.*

Let formed matrix $T = [T_1, T_2] \in E^{p\times m}$, where $T_1 \in E^{p\times l}$, $T_2 \in E^{p\times t}$. Perform elementary row (column) operations to obtain the Smith form

$$S_T = T_L T T_R, \tag{1}$$

where $T_L \in E^{p\times p}$, $T_R \in E^{m\times m}$.

Suppose $T_R \in E^{m\times m}$ is a right unimodular matrix. Then by definition, structure $S_T = [I_p \quad 0_{p,m-p}]$, and we obtain

$$\begin{aligned} S_T &= T_L T T_R, \\ T T_R &= T_L^{-1} S_T \\ &= T_L^{-1}[I_p \quad 0_{p,m-p}] \\ &= T_{GL}[I_p \quad 0_{p,m-p}] \\ &= [T_{GL} \quad 0_{p,m-p}], \end{aligned} \tag{2}$$

where $T_{GL} \in E^{p\times p}$. We define $T_R^{-1} = \hat{T} \in E^{m\times m}$ with $\hat{T}$ as:

$$\hat{T} = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$$

with $A \in E^{p\times l}$, $B \in E^{p\times t}$, $C \in E^{(m-p)\times l}$, $D \in E^{(m-p)\times t}$.

$$\begin{aligned} T &= [T_1 \quad T_2] \\ &= [T_{GL} \quad 0_{p,m-p}]T_R^{-1} \\ &= T_{GL}[I_p \quad 0_{p,m-p}]\begin{bmatrix} A & B \\ C & D \end{bmatrix} \\ &= T_{GL}[A \quad B], \end{aligned}$$

where $[A \quad B] \in E^{p\times m}$ is the right unimodular and $T_{GL} = T_L'$ is the left structure matrix of T:

$$[T_1 \quad T_2] = T_{GL}[A \quad B]$$

$$T_1 = T_{GL}A \text{ and } T_2 = T_{GL}B.$$

That is, T_{GL} is the left common divisor of T_1 and T_2. Define T_R as

$$T_R = \begin{bmatrix} T_{R1} & T_{R2} \\ T_{R3} & T_{R4} \end{bmatrix}.$$

Then from equation (2), we obtain

$$TT_R = [T_{GL} \quad 0_{p,m-p}],$$

$$[T_1 \quad T_2]\begin{bmatrix} T_{R1} & T_{R2} \\ T_{R3} & T_{R4} \end{bmatrix} = [T_{GL} \quad 0_{p,m-p}],$$

$$[T_1T_{R1} + T_2T_{R3} \quad T_1T_{R2} + T_2T_{R4}] = [T_{GL} \quad 0_{p,m-p}],$$

and thus

$$T_1T_{R1} + T_2T_{R3} = T_{GL}. \tag{3}$$

Let $\overline{T}_L \in E^{p\times p}$ be any other left common divisor of T_1 and T_2. Then

$$T_1 = \overline{T}_L F \text{ and } T_2 = \overline{T}_L G, \tag{4}$$

where $F \in E^{p\times l}$, $G \in E^{p\times t}$. Then from (3) and (4), we obtain

$$\begin{aligned} T_1 T_{R1} + T_2 T_{R3} &= \overline{T}_L F T_{R1} + \overline{T}_L G T_{R3} \\ &= \overline{T}_L [F T_{R1} + G T_{R3}] \\ &= T_{GL}. \end{aligned}$$

We see that T_{GL} is multiple of any other common left divisor $(\overline{T}_L)$. This means T_{GL} is a greatest common left divisor of T_1 and T_2.

And in the same way, we can find the right greatest common divisor. From the above description, the following theorem is obtained.

Theorem 14. *If T_{GL} is a greatest common left divisor of T_1 and T_2, then any other greatest common left divisor $(\overline{T}_{GL})$ is a multiple of T_{GL}, i.e.,*

$$\overline{T}_{GL} = T_{GL} U,$$

where $U \in E^{p\times p}$ is unimodular.

Definition 15. $T_1 \in E^{p\times l}$ and $T_2 \in E^{p\times t}$ with $l + t \geq p = \operatorname{rank}[T_1 \;\; T_2]$ are called *left coprime* if their greatest common left divisor is unimodular. Likewise $T_1 \in E^{l\times m}$ and $T_2 \in E^{t\times m}$ with $l + t \geq m = \operatorname{rank}\begin{bmatrix} T_1 \\ T_2 \end{bmatrix}$ is called *right coprime* if their greatest common right divisor is unimodular.

Theorem 16. *Let $T_1 \in E^{p\times l}$ and $T_2 \in E^{p\times t}$ with $l + t = m \geq p =$ rank $[T_1 \;\; T_2]$. Then the following statements are equivalent*:

(1) *T_1 and T_2 are left coprime.*

(2) *The ED-matrix $T = [T_1 \;\; T_2] \in E^{p\times m}$ has no zeros in $\mathbb{C}$.*

(3) *There exists a unimodular matrix* $\overline{T}_R \in E^{m\times m}$ *such that*

$$[T_1 \;\; T_2]\overline{T}_R = [I_p \;\; 0_{p,\, m-p}] \equiv S_T,$$

where $S_T \in E^{p\times m}$ *is the Smith form of T.*

(4) *There exists* $Y \in E^{l\times p}$, $Z \in E^{t\times p}$ *such that*

$$T_1 Y + T_2 Z = I_p.$$

(5) *There exists* $T_3 \in E^{(m-p)\times l}$, $T_4 \in E^{(m-p)\times t}$ *such that*

$$\begin{bmatrix} T_1 & T_2 \\ T_3 & T_4 \end{bmatrix} \in E^{m\times m} \text{ unimodular}.$$

Example 17. This example shows how to use left structure matrix and the greatest common left divisor of two matrices polynomials (the set of all polynomials is a Euclidean domain) that have the same number of rows, namely $T_1(x) \in \mathbb{R}[x]^{2\times 3}$ and $T_2(x) \in \mathbb{R}[x]^{2\times 1}$. Suppose

$$T_1(x) = \begin{bmatrix} x & 0 & x+1 \\ 0 & (x+1)^2 & x \end{bmatrix},\; T_2(x) = \begin{bmatrix} 0 \\ x+2 \end{bmatrix}.$$

Then

$$\begin{aligned} T(x) &= [T_1(x), T_2(x)] \\ &= \begin{bmatrix} x & 0 & x+1 & 0 \\ 0 & (x+1)^2 & x & x+2 \end{bmatrix}. \end{aligned}$$

By performing elementary row (column) operation, we obtain Smith form of $T(x)$, as follows:

$$S_T(x) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

With elementary row operation matrix, $T_L(x)^{-1} = \begin{bmatrix} 1 & 0 \\ x & 1 \end{bmatrix}$ and with elementary column operation matrix,

$$T_R(x)^{-1} = \begin{bmatrix} x & 0 & x+1 & 0 \\ -x^2 & (x+1)^2 & -x^2 & x+2 \\ 1 & 0 & 1 & 0 \\ -x+2 & x & -x+2 & 1 \end{bmatrix}$$

such that $T(x) = T_L(x)^{-1} S_T(x) T_R(x)^{-1}$. Based on Theorem 10, structure matrix of $T_1(x)$ and $T_2(x)$ is,

$$T_L'(x) = T_L(x)^{-1} \begin{bmatrix} D(x) \\ 0_{p-r,r} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 \\ x & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 \\ x & 1 \end{bmatrix},$$

$$T_R'(x) = [D(x) \quad 0_{r,m-r}] T_R(x)^{-1}$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} x & 0 & x+1 & 0 \\ -x^2 & (x+1)^2 & -x^2 & x+2 \\ 1 & 0 & 1 & 0 \\ -x+2 & x & -x+2 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} x & 0 & x+1 & 0 \\ -x^2 & (x+1)^2 & -x^2 & x+2 \end{bmatrix}.$$

So a greatest common divisor of $T_1(x)$ and $T_2(x)$ is

$$T_L'(x) = \begin{bmatrix} 1 & 0 \\ x & 1 \end{bmatrix}$$

which is the greatest common left divisor.

Example 18. Consider a Euclidean domain of proper rational functions $\mathbb{R}_{pr}(x)$ with a discrete valuation

$$\delta_\infty(\cdot) : \mathbb{R}(x) \to Z \cup \{\infty\},$$

given by $\delta_\infty(t(x)) := \deg d(x) - \deg n(x)$ and $\delta_\infty(0) := +\infty$, if $t(x) = \dfrac{n(x)}{d(x)} \in \mathbb{R}(x)$, $d(x) \neq 0$ (Vardulakis [3]).

Let $A = \begin{pmatrix} \frac{1}{x} & 0 \\ \frac{x+1}{x} & 1 \end{pmatrix}$, $B = \begin{pmatrix} \frac{1}{x^2} \\ \frac{x+1}{x^3+1} \end{pmatrix}$ and $T(x) = \begin{pmatrix} \frac{1}{x} & 0 & \frac{1}{x^2} \\ \frac{x+1}{x} & 1 & \frac{x+1}{x^3+1} \end{pmatrix}$.

Find the Smith form of $T(x)$.

Bring the element of least $\delta_\infty(\cdot)$ to position $(1, 1)$,

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \frac{1}{x} & 0 & \frac{1}{x^2} \\ \frac{x+1}{x^3} & 1 & \frac{x+1}{x^3+1} \end{pmatrix} = \begin{pmatrix} \frac{x+1}{x^3} & 1 & \frac{x+1}{x^3+1} \\ \frac{1}{x} & 0 & \frac{1}{x^2} \end{pmatrix}.$$

Change the first column to second column

$$\begin{pmatrix} \frac{x+1}{x^3} & 1 & \frac{x+1}{x^3+1} \\ \frac{1}{x} & 0 & \frac{1}{x^2} \end{pmatrix}\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \frac{x+1}{x^3} & \frac{x+1}{x^3+1} \\ 0 & \frac{1}{x} & \frac{1}{x^2} \end{pmatrix}.$$

Write $\dfrac{x+1}{x^3} = \dfrac{1}{x} \cdot \dfrac{x+1}{x^2}$. Add $-\dfrac{x+1}{x^2}$ times the second row to the first row

$$\begin{pmatrix} 1 & -\frac{x+1}{x^2} \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & \frac{x+1}{x^3} & \frac{x+1}{x^3+1} \\ 0 & \frac{1}{x} & \frac{1}{x^2} \end{pmatrix} = \begin{pmatrix} 1 & 0 & \frac{x^5 - x^3 - x - 1}{x^4(x^3+1)} \\ 0 & \frac{1}{x} & \frac{1}{x^2} \end{pmatrix}.$$

Add $-\dfrac{x^5-x^3-x-1}{x^4(x^3+1)}$ times the first column to the third column

$$\begin{pmatrix} 1 & 0 & \dfrac{x^5-x^3-x-1}{x^4(x^3+1)} \\ 0 & \dfrac{1}{x} & \dfrac{1}{x^2} \end{pmatrix}\begin{pmatrix} 1 & 0 & -\dfrac{x^5-x^3-x-1}{x^4(x^3+1)} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \dfrac{1}{x} & \dfrac{1}{x^2} \end{pmatrix}.$$

Add $-\dfrac{1}{x}$ times the second column to the third column

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \dfrac{1}{x} & \dfrac{1}{x^2} \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -\dfrac{1}{x} \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \dfrac{1}{x} & 0 \end{pmatrix}.$$

So after multiplying all of elementary matrices, we have

$$\begin{pmatrix} 0 & 1 \\ 1 & -\dfrac{x+1}{x^2} \end{pmatrix}\begin{pmatrix} \dfrac{1}{x} & 0 & \dfrac{1}{x^2} \\ \dfrac{x+1}{x} & 1 & \dfrac{x+1}{x^3+1} \end{pmatrix}\begin{pmatrix} 0 & 1 & -\dfrac{1}{x} \\ 1 & 0 & -\dfrac{x^5-x^3-x-1}{x^4(x^3+1)} \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \dfrac{1}{x} & 0 \end{pmatrix}.$$

And

$$\begin{pmatrix} \dfrac{1}{x} & 0 & \dfrac{1}{x^2} \\ \dfrac{x+1}{x} & 1 & \dfrac{x+1}{x^3+1} \end{pmatrix} = \begin{pmatrix} \dfrac{x+1}{x^2} & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & \dfrac{1}{x} & 0 \end{pmatrix}\begin{pmatrix} \dfrac{x+1}{x} & -1 & \dfrac{x+1}{x^2} \\ 0 & 0 & \dfrac{x-1}{x} \\ 0 & \dfrac{x}{x+1} & 0 \end{pmatrix}^{-1}.$$

So the greatest common left divisor of $A = \begin{pmatrix} \dfrac{1}{x} & 0 \\ \dfrac{x+1}{x} & 1 \end{pmatrix}$ and $B = \begin{pmatrix} \dfrac{1}{x^2} \\ \dfrac{x+1}{x^3+1} \end{pmatrix}$

is $\begin{pmatrix} \dfrac{x+1}{x^2} & \dfrac{1}{x} \\ 1 & 0 \end{pmatrix}$.

4. Conclusion

Based on the results and discussion, the following is concluded:

(1) If $T \in E^{p\times m}$ with rank $T = r$, then the left structure matrix of T is defined as $T_L' = T_L^{-1}\begin{bmatrix} D \\ 0_{p-r,r} \end{bmatrix}$, where $T_L^{-1} \in E^{p\times p}$ is the inverse of a number of elementary row operations on T.

(2) If $T \in E^{p\times m}$ with rank $T = r$, then the right structure matrix of T is defined as $T_R' = [D \quad 0_{r,m-r}]T_R^{-1}$, where $T_R \in E^{m\times m}$ is the inverse of a number of elementary column operations on T.

(3) Let $T_1 \in E^{p\times l}$, $T_2 \in E^{p\times t}$ form $T = [T_1 \quad T_2] \in E^{p\times m}$ with $l + t = m \geq p = \operatorname{rank} T$. Then the greatest common left divisor of T_1 and T_2 is the left structure matrix of T in the form $T_L' \in E^{p\times p}$.

(4) Let $T_1 \in E^{l\times m}$, $T_2 \in E^{t\times m}$ form $T = \begin{bmatrix} T_1 \\ T_2 \end{bmatrix} \in E^{p\times m}$ with $l + t = p \geq m = \operatorname{rank} T$. Then the greatest common right divisor of T_1 and T_2 is the right structure matrix of T in the form $T_R' \in E^{m\times m}$.

(5) Steps to obtain the greatest common (left/right) divisor of two matrices:

(a) If both matrices A and B have the same number of rows, then form $[A \quad B]$. And if both matrices A and B have the same number of columns, then form $\begin{bmatrix} A \\ B \end{bmatrix}$.

(b) Use elementary operations on $[A \quad B]$ or on $\begin{bmatrix} A \\ B \end{bmatrix}$ to obtain the Smith form.

(c) By using the Smith form, find structure matrix for $\begin{bmatrix} A & B \end{bmatrix}$ or $\begin{bmatrix} A \\ B \end{bmatrix}$ as parts (1) and (2).

The greatest common divisor of matrix $\begin{bmatrix} A & B \end{bmatrix}$ is the left of structure matrix. And the greatest common divisor of matrix $\begin{bmatrix} A \\ B \end{bmatrix}$ is the right of the structure matrix.

Acknowledgement

The authors thank the anonymous referees for their valuable suggestions which led to the improvement of the manuscript.

References

[1] A. I. G. Vardulakis, Structure and Smith-McMillan form of a rational matrix at infinity, International Journal Control 35 (1982), 701-725.

[2] A. I. Vardulakis, Divisors and greatest common divisors of polynomial matrices, Linear Multivariable Control, John Wiley and Sons, New Delhi, 1991, pp. 16-18.

[3] A. I. Vardulakis, Linear Multivariable Control, Thomson Press, New Delhi, 1991.

[4] F. R. Gantmacher, The Theory of Matrices, Chelsea Publishing Company, New York, 1959.

[5] J. B. Fraleigh, A First Course in Abstract Algebra, Fifth Edition, Addison-Wesley Publishing Company, 1994.

[6] L. Pernebo, Algebraic Theory for Linear Multivariable Systems, Department of Automatic Control, Lund Institute of Technology, Sweden, 1978.

[7] M. Solak, A note on the Wolovich method of extraction of a greatest common divisor of two polynomial matrices, IEEE Transactions on Automatic Control, 1985, pp. 1032-1033.

[8] M. Vidyasagar, Control System Synthesis: A Factorization Approach, The MIT Press Cambridge, London, 1985.

[9] N. Erawaty, Pemanfaatan Bentuk Smith-McMillan untuk Parameterisasi Kompensator yang Menstabilkan Plant Proper, Institut Teknologi Bandung, Bandung, 2000.

[10] N. L. Thomsen, A Euclidean Algorithm for Integer Matrices, American Mathematical Monthly 122 (2015).

[11] R. Howard, The Smith normal form, Ring, Determinants and the Smith Normal Form, University of South Caroline, Columbia, 2005, pp. 52-64.

[12] R. R. Bitmead, Greatest common divisor via generalized Sylvester and Bezout matrices, IEEE Transactions on Automatic Control AC-23(6) (1978), 1043-1047.

[13] S. B. Cameron, Introduction to Mathematical Control Theory, Oxford University Press, Oxford, 1985.

[14] S. Barnett, Regular greatest common divisor of two polynomial matrices, Mathematical Proceedings of the Cambridge Philosophical Society, 1972, pp. 161-165.

[15] S. D. Prugsapitak, Complete residue system in the ring of matrices over Euclidean domains and a greatest common divisor of matrices, Int. J. Pure Appl. Math. 87(3) (2013), 421-430.

[16] T. Glad, Linear Systems, Lingkoping Universitet, Linkoping Sweden, 2012.

[17] A. A. Howard, Elementary Linear Algebra, Ninth Edition, United States of America, John Wiley & Sons, Inc., 2005.