Matrix Representation of the Shifting Operation and Numerical Properties of the ERES Method for Computing the Greatest Common Divisor of Sets of Many Polynomials

D. Christou[a,*], N. Karcanias[a], M. Mitrouli[b]

[a]*Systems and Control Centre, School of Engineering and Mathematical Sciences, City University, Northampton Square, EC1V 0HB, London, United Kingdom.*
[b]*Department of Mathematics, University of Athens, Panepistemiopolis 15773, Athens, Greece.*

Abstract

The *Extended-Row-Equivalence and Shifting (ERES) method* is a matrix-based method developed for the computation of the greatest common divisor (GCD) of sets of many polynomials. In this paper we present the formulation of the *shifting operation* as a matrix product which allows us to study the fundamental theoretical and numerical properties of the ERES method by introducing its complete algebraic representation. Then, we analyse in depth its overall numerical stability in finite precision arithmetic. Numerical examples and comparison with other methods are also presented.

Keywords: Univariate real polynomials, Greatest common divisor, Shifting operation, Numerical stability.

1. Introduction

The computation of the greatest common divisor (GCD) of polynomials is an algebraic problem which has been studied intesively for many years. The algorithm associated with Euclid's division method [1] is the oldest known solution to this problem. The computational methods for computing the GCD of real univariate polynomials can be separated in two main categories:

a) The *Euclidean type methods* which rely on Euclid's division algorithm and its variations.
b) The *matrix-based methods* which are based on the processing of a matrix formed directly from the coefficients of the given polynomials.

The matrix-based methods may be further classified to those that:

i) form a matrix for two polynomials and work on pairwise computations iteratively,

[*] Corresponding author
Email addresses: dchrist@math.uoa.gr (D. Christou), N.Karcanias@city.ac.uk (N. Karcanias), mmitroul@math.uoa.gr (M. Mitrouli)

Preprint submitted to Elsevier *June 30, 2013*

ii) form a matrix that corresponds to the whole set of polynomials and process it either directly or iteratively.

Early GCD algorithms were developed using Euclidean-based methods, applied to two polynomials [2, 3, 4]. The Euclidean algorithm is efficient when the polynomials have integer coefficients, but it becomes inefficient when the polynomials have coefficients from the field of real numbers due to the use of finite precision arithmetic, which introduces numerical errors into the solution. In 1985, Schönhage introduced the notion of *Quasi-GCD* [5], and in 1989, Noda and Sasaki described a special version of Euclid's algorithm for computing the GCD of a pair of coprime polynomials with inexact coefficients [6]. This approach is amongst the first attempts to define and compute an approximate GCD of polynomials by means of symbolic-numeric computations. The development of numerical stable GCD algorithms which can deal with polynomials of inexact data has attracted a lot of attention the past thirty years and several methods have been proposed [7, 8, 9, 10, 11, 12, 13, 14, 15, 16]. The various techniques, which have been developed for the computation of *approximate* solutions, are based on methodologies where exact properties of these notions are relaxed and appropriate solutions are sought by using a variety of numerical tests.

The use of finite precision arithmetic in computer algebra makes the extension of the Euclidean algorithm to sets of many polynomials a rather difficult task. The iterative application of the Euclidean algorithm to two polynomials at a time often results in a total numerical error which might exceed the machine's fixed numerical tolerance. Conversely, the developed matrix-based methods tend to be more effective in handling sets of several polynomials and producing solutions of better numerical quality. The use of matrices in the problem of computing the GCD of many polynomials appears early in Barnett's work [17, 18, 19], who developed a technique for computing the degree and the coefficients of the GCD by using companion and Sylvester matrices.

In [20], Karcanias (1987) has shown that the GCD is an invariant of the row space of the basis matrix of the set of polynomials, as well as that it is also an invariant under the shifting operation. This has led to the development of the current approach that avoids the use of Euclidean divisions. The *Extended-Row-Equivalence and Shifting* (ERES) method [21] is an iterative matrix-based method developed for the computation of the greatest common divisor (GCD) of sets of real polynomials in one variable. The method exploits the invariance of the greatest common divisor of a set of many polynomials under elementary row transformations and partial column shifting by transforming a basis matrix, which is formed directly from the coefficients of the polynomials of a given set, into a simpler matrix containing the vector of coefficients of the GCD. The previous study of its theoretical and numerical properties in [20, 21, 22] revealed the advantage of the ERES method to handle large sets polynomials and to invoke an efficient termination criterion that allows the computation of approximate solutions when the initial data have numerical inaccuracies [23]. The development of the ERES method as it has been described in [21] is an inherently robust algebraic method which defines a special matrix equivalence. However, the complete algebraic representation of the method remained an open issue due to its iterative nature and the luck of an algebraic expression for the partial column shifting transformation, referred to as the *shifting operation.* The aim is to establish an algebraic relationship between the initial basis matrix of a given set of several polynomials and the last matrix which occurs after the iterative application of the ERES operations and provides the GCD. Apart from its theoretical value, this algebraic representation is significant for the complete analysis of the overall numerical stability of the ERES method which could not be studied before. The main objectives of this paper are: a) to present the general algebraic representation of the ERES method and discuss its theoretical and practical use, and b) to analyse the overall numerical stability of the method in finite-precision arithmetic.

The paper is structured as follows:

In Section 2, the definition and the most important properties of the ERES operations are presented and we give a brief description of how the ERES method is formulated. In Section 3 the major issue of having a matrix representation for the shifting operation is analysed and discussed. The results from the study of the shifting operation are used in Section 4 in order to introduce the general algebraic representation of the ERES method which eventually establishes the ERES representation of the GCD of a set of many polynomials. This representation forms the basis for the analysis of the overall numerical stability of the method in Section 5. Numerical examples and comparison with other methods are also presented.

Notation. In the following, $\mathbb{N}$ and $\mathbb{R}$ denote the sets (fields) of natural and real numbers, respectively. $\mathbb{R}[s]$ denotes the ring of polynomials in one variable over $\mathbb{R}$. Capital letters denote matrices and small underlined letters denote vectors. By $p(s)$ we denote a polynomial in s with real coefficients. The greatest common divisor of a set $\mathcal{P}$ will be denoted by $\gcd\{\mathcal{P}\}$. The following list includes the basic notations that are used in the document.

$A \in \mathbb{R}^{m \times n}$	Matrix A with elements from $\mathbb{R}$ arranged in m rows and n columns ($m, n \in \mathbb{N}$ and $m, n \geq 2$).
$\underline{v} \in \mathbb{R}^m$	Column vector with $m \geq 2$ elements from $\mathbb{R}$.
A^t	Transpose matrix of A.
$\underline{v}^t$	Transpose vector of $\underline{v}$.
$\rho(A)$	The rank of a matrix A.
$\deg\{p(s)\}$	The degree of a polynomial $p(s)$.
$\|\underline{v}\|_2$	The Euclidean norm of $\underline{v}$: $\|\underline{v}\|_2 = \sqrt{\sum_{i=1}^{\mu} \|v_i\|^2}$
$\|A\|_2$	The Euclidean norm of A : $\|A\|_2 = \sqrt{\text{max eigenvalue of } A^t A}$
$\|A\|_\infty$	The infinity norm of A : $\|A\|_\infty = \max_{1 \leq i \leq \mu} \sum_{j=1}^{\nu} \|a_{ij}\|$
$\triangleq$	Mathematical operator which denotes equality by definition.
$:=$	Mathematical operator which denotes equality by input.
$\approx$	Mathematical operator which denotes approximate equality.

2. Definition of the ERES operations and background results

2.1. Background theory

Consider the set of real polynomials in one variable (univariate polynomials):

$$\mathcal{P}_{m,n} = \Big\{ p_i(s) \in \mathbb{R}[s],\ i = 1, 2, \ldots, m \text{ with } n = \max_i \left(\deg\{p_i(s)\} \geq 1 \right) \Big\} \tag{1}$$

We represent the polynomials $p_i(s)$ with respect to the highest degree n as

$$p_i(s) = a_{i,n}s^n + a_{i,n-1}s^{i,n-1} + \ldots + a_{i,1}s + a_{i,0}\ ,\ a_{i,n} \neq 0,\ i = 1, 2, \ldots, m \quad (2)$$

Definition 1. For any $\mathcal{P}_{m,n}$ set, we define a vector representative (vr), $\underline{p}_m(s)$ and a basis matrix P_m represented as

$$\underline{p}_m(s) = [\, p_1(s), \ldots, p_m(s)\,]^t = [\,\underline{p}_1, \ldots, \underline{p}_{m-1}, \underline{p}_m\,] \cdot \underline{e}_n(s) = P_m \cdot \underline{e}_n(s),$$

where $P_m \in \mathbb{R}^{m\times(n+1)}$, $\underline{e}_n(s) = [1, s, \ldots, s^{n-1}, s^n]^t$ and $\underline{p}_i \in \mathbb{R}^{n+1}$ for all $i = 1, \ldots, m$.

The matrix P_m is formed directly from the coefficients of the polynomials of the set $\mathcal{P}_{m,n}$ and it has the least possible dimensions.

Definition 2. If c is the integer for which $\underline{p}_1 = \ldots = \underline{p}_{c-1} = \underline{0}$ and $\underline{p}_c \neq 0$, then $c = w(\mathcal{P}_{m,n})$ is called the *order* of $\mathcal{P}_{m,n}$ and s^c is an elementary divisor of the GCD. The set $\mathcal{P}_{m,n}$ is considered to be a c-order set and will be called *proper* if $c = 0$, and *nonproper* if $c \geq 1$.

For a nonproper set $\mathcal{P}_{m,n}$ with $w(\mathcal{P}_{m,n}) = c$, we can always consider the corresponding proper one $\mathcal{P}_{m,\,n-c}$ by dismissing the c leading zero columns. Then $\gcd\{\mathcal{P}_{m,n}\} = s^c \cdot \gcd\{\mathcal{P}_{m,\,n-c}\}$. In the following without loss of generality we assume that $\mathcal{P}_{m,n}$ is proper.

Definition 3 (ERES operations). Given a set $\mathcal{P}_{m,n}$ of many polynomials with a basis matrix P_m the following operations are defined [20] :

a) Elementary row operations with scalars from $\mathbb{R}$ on P_m.
b) Addition or elimination of zero rows on P_m.
c) If $\underline{a}^t = [0, \ldots, 0, a_l, \ldots, a_{n+1}] \in \mathbb{R}^{n+1}$, $a_l \neq 0$ is a row of P_m then we define as the *shifting* operation

$$\textit{shf} : \mathrm{shf}(\underline{a}^t) = [a_l, \ldots, a_{n+1}, 0, \ldots, 0] \in \mathbb{R}^{n+1}$$

By $\mathrm{shf}(\mathcal{P}_{m,n})$, we shall denote the set obtained from $\mathcal{P}_{m,n}$ by applying shifting on every row of P_m (matrix shifting).

Type (a), (b) and (c) operations are referred to as *Extended-Row-Equivalence and Shifting (ERES) operations.* The ERES operations without applying the shifting operation are referred to as *ERE operations.*

The following theorem describes the properties characterising the GCD of any given $\mathcal{P}_{m,n}$.

Theorem 1 ([20]). *For any set $\mathcal{P}_{m,n}$, with a basis matrix P_m, $\rho(P_m) = r$ and $\gcd\{\mathcal{P}_{m,n}\} = \phi(s)$ we have the following properties:*

i) If $\mathcal{R}_P$ is the row space of P_m, then $\phi(s)$ is an invariant of $\mathcal{R}_P$ (e.g. $\phi(s)$ remains invariant after the execution of elementary row operations on P_m). Furthermore if $r = \dim(\mathcal{R}_P) = n + 1$, then $\phi(s) = 1$.

ii) If $w(\mathcal{P}_{m,n}) = c \geq 1$ and $\mathcal{P}^*_{m,n} = \mathrm{shf}(\mathcal{P}_{m,n})$, then

$$\phi(s) = \gcd\{\mathcal{P}_{m,n}\} = s^c \cdot \gcd\left\{\mathcal{P}^*_{m,n}\right\}$$

iii) If $\mathcal{P}_{m,n}$ is proper, then $\phi(s)$ is invariant under the combined ERES set of operations.

2.2. The formulation of the ERES method and the computation of the GCD of a set of polynomials

ERES operations preserve the GCD of any $\mathcal{P}_{m,n}$ and thus can be easily applied iteratively in order to obtain a modified basis matrix with much simpler structure [20]. The ERES method in its simplest form consists of three basic procedures:

1. Construction of the proper basis matrix P_m for the set $\mathcal{P}_{m,n}$.
2. Application of elementary row operations to the processed matrix, which practically involves row reordering, triangularization, and elimination of zero rows (ERE operations).
3. Application of the shifting operation to the nonzero rows of the processed matrix.

After successive applications of the ERES operations to the initial basis matrix, the maximal degree of the given set of polynomials is reduced, and after a finite number of steps the resulting matrix has rank 1. At this point, the process is terminated and, considering that all the arithmetic operations are performed accurately (e.g. by using symbolic-rational operations), any row of the last matrix specifies the coefficients of the GCD of the set. The iterative application of the processes of triangularization and shifting forms the core of the ERES method and we shall refer to it as the *main procedure* of the method.

The main problem in the formulation of an algebraic expression, which will establish the connection between the initial basis matrix P_m and the final matrix that contains the coefficients of the GCD, requires appropriate matrix representations of the ERE operations and the shifting operation, respectively. The ERE row operations, i.e. triangularization, deletion of zero rows and reordering of rows, can be represented [24, 25] by a matrix $R \in \mathbb{R}^{r \times m}$, $r < m$, which converts the initial rectangular matrix P_m into an upper trapezoidal form. Conversely, the matrix representation of the shifting operation is not straightforward. The problem of the matrix representation of the shifting operation for real matrices has remained open until now. Solving this problem is crucial for establishing a general matrix representation of the ERES method for all the performed iterations. Therefore, in the following section we aim to find the simplest possible algebraic relation between a matrix and its shifted form.

3. The *shifting* operation for real matrices

The *shifting operation* is a special matrix transformation which is not very common in the literature of algebra. In Definition 3 the shifting operation is defined for real vectors as a permutation of consecutive zero elements. Specifically, having a real vector

$$\underline{a} = [\underbrace{0, \ldots, 0}_{k \text{ elements}}, a_{k+1}, \ldots, a_n] \in \mathbb{R}^n, \; a_{k+1} \neq 0$$

the shifting operation is defined as

$$shf : \mathrm{shf}(\underline{a}) = [a_{k+1}, \ldots, a_n, 0, \ldots, 0] \in \mathbb{R}^n$$

This definition can be extended to the case of real matrices.

Definition 4. Given a matrix $A = [\underline{a}_1, \underline{a}_2, \ldots, \underline{a}_m]^t \in \mathbb{R}^{m \times n}$, where $\underline{a}_i \in \mathbb{R}^n$ for $i = 1, 2, \ldots, m$ are the row-vectors of A, the shifting operation for matrices is defined as the application of vector-shifting to every row of A. This transformation will be referred to as *matrix-shifting* and the shifted form of A will be denoted by

$$\operatorname{shf}(A) \triangleq A^* = [\operatorname{shf}(\underline{a}_1), \operatorname{shf}(\underline{a}_2), \ldots, \operatorname{shf}(\underline{a}_m)]^t \in \mathbb{R}^{m \times n}$$

It is important to notice that the shifting operation, as defined here, permutes the elements of a vector without changing their values, and this is a basic requirement for the shifting operation in the study of the numerical properties of the ERES method. The vector-shifting can be represented by the multiplication:

$$\operatorname{shf}(\underline{a}) = \underline{a} \cdot J_{k,n}$$

where $J_{k,n}$ is an appropriate $n \times n$ permutation matrix which is a square binary matrix that has exactly one entry 1 in each row and each column, and zeros elsewhere. Each such matrix represents a specific permutation of k elements and for the vector-shifting it has the form:

$$J_{k,n} = \left[\begin{array}{c|c} O_{n-k} & I_k \\ I_{n-k} & O_k \end{array} \right] \in \mathbb{R}^{n \times n} \tag{3}$$

where I_i denotes the $i \times i$ identity matrix and O_i denotes the $i \times i$ zero matrix for $i = k,\ n-k$.

Although it is rather simple to represent the vector-shifting transformation with a simple vector-matrix multiplication, it is not obvious how to represent the matrix-shifting transformation, because in general the application of vector-shifting to the rows of a matrix alters the structure of the columns in a non-uniform way. The problem of representing the matrix-shifting by using an appropriate matrix-matrix multiplication is challenging for the study of the theoretical and numerical properties of the ERES method. We are particularly interested in finding an algebraic relationship between a real matrix and its shifted form in the class of upper trapezoidal matrices. This type of matrices occurs after applying Gaussian elimination, or other triangularization method, and they have the following generic form:

$$A = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1m} & \ldots & a_{1n} \\ 0 & a_{22} & \ldots & a_{2m} & \ldots & a_{2n} \\ \vdots & \ddots & \ddots & \vdots & \vdots & \vdots \\ 0 & \ldots & 0 & a_{mm} & \ldots & a_{mn} \end{bmatrix} \in \mathbb{R}^{m \times n}, \quad m < n \tag{4}$$

Then, the shifted form of A, which is obtained by the matrix-shifting transformation as defined in Definition 4, is

$$A^* = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1m} & \ldots & a_{1n} \\ a_{22} & \ldots & a_{2m} & \ldots & a_{2n} & 0 \\ \vdots & \vdots & \vdots & \iddots & \iddots & \vdots \\ a_{m\,m} & \ldots & a_{m\,n} & 0 & \ldots & 0 \end{bmatrix} \in \mathbb{R}^{m \times n}, \quad m < n \tag{5}$$

Definition 5. a) If $A = [\underline{a}_1, \underline{a}_2, \ldots, \underline{a}_m]^t \in \mathbb{R}^{m\times n}$, then we can define the matrices $A_i = [\underline{0}, \ldots, \underline{a}_i, \ldots \underline{0}]^t \in \mathbb{R}^{m\times n}$, for every $i = 1, 2, \ldots, m$, such that

$$A = \sum_{i=1}^{m} A_i \tag{6}$$

where $\underline{a}_i$ is the i^{th} row of A and $\underline{0} \in \mathbb{R}^n$ is a n-dimensional zero vector.

b) We define the permutation matrices $J_i \in \mathbb{R}^{n\times n}$ for $i = 1, 2, \ldots, m$, so that every J_i gives the appropriate shifting to each A_i respectively. Therefore,

$$\text{shf}(A) = \sum_{i=1}^{m} A_i \, J_i \tag{7}$$

Since $a_{11} \neq 0$, we note that $J_1 = I_n$, where I_n is the $n \times n$ identity matrix.

Remark 1. If A has full rank, then, since it is defined as an upper trapezoidal matrix with $a_{ii} \neq 0$ for all $i = 1, \ldots, m$, it is right-invertible. Let us denote its right inverse by $A_r^{-1} \in \mathbb{R}^{n\times m}$. Hence, $A\, A_r^{-1} = I_m$.

The following theorem establishes the connection between a nonsingular upper trapezoidal matrix and its shifted form.

Theorem 2. *If $A \in \mathbb{R}^{m\times n}$, $2 \leq m < n$, is a non-singular upper trapezoidal matrix with rank $\rho(A) = m$ and $\text{shf}(A) \in \mathbb{R}^{m\times n}$ is the matrix obtained from A by applying shifting to its rows, then there exists a square matrix $S \in \mathbb{R}^{n\times n}$ such that:*

$$\text{shf}(A) = A \cdot S \tag{8}$$

The matrix S will be referred to as the shifting matrix of A.

Proof. Let $A^* = \text{shf}(A)$. We shall use the notation described in Definition 5 and we will follow the next method to determine the shifting matrix $S \in \mathbb{R}^{n\times n}$.

1. Apply to the original matrix A the $n \times n(m+1)$ block matrix:

$$S^{(1)} = \begin{bmatrix} J_1 & \ldots & J_m & A_r^{-1} \end{bmatrix} \tag{9}$$

such that:

$$A^{(1)} = A \cdot S^{(1)}$$

2. Multiply the matrix $A^{(1)}$ by the $n(m+1) \times mn$ block matrix:

$$S^{(2)} = \begin{bmatrix} I_n & O_n & \ldots & O_n \\ O_n & I_n & \ldots & O_n \\ \vdots & \vdots & \ddots & \vdots \\ O_n & O_n & \ldots & I_n \\ (A_1 - A)\, J_1 & (A_2 - A)\, J_2 & \ldots & (A_m - A)\, J_m \end{bmatrix} \tag{10}$$

where O_n denotes the $n \times n$ zero matrix and I_n the $n \times n$ identity matrix. Hence,

$$A^{(2)} = A^{(1)} \cdot S^{(2)}$$

3. Multiply the matrix $A^{(2)}$ by the $mn \times n$ block matrix:

$$S^{(3)} = \begin{bmatrix} I_n \\ \vdots \\ I_n \end{bmatrix} \tag{11}$$

and hence,

$$A^{(3)} \triangleq A^* = A^{(2)} \cdot S^{(3)}$$

The final matrix $S = S^{(1)} \cdot S^{(2)} \cdot S^{(3)}$ has the form:

$$S = \sum_{i=1}^{m} \left(I_n - A_r^{-1} A + A_r^{-1} A_i \right) J_i \tag{12}$$

and satisfies the equation: $A^* = A \cdot S$ □

In the proof of Theorem 2 the right inverse matrix A_r^{-1} of A is not unique when $m < n$. Conversely, the pseudo-inverse matrix $A^\dagger \in \mathbb{R}^{n \times m}$ of A can be uniquely determined by calculating the singular value decomposition of A [25], such that

$$A\, A^\dagger = I_m$$

Therefore, an alternative expression of the representation (12) of the shifting matrix S can be given, if we use the pseudo-inverse matrix of A. This is

$$S = \sum_{i=1}^{m} \left(I_n - A^\dagger A + A^\dagger A_i \right) J_i \tag{13}$$

and it is more appropriate for the numerical computation of the shifting matrix.

Example 1. Consider the following randomly selected matrix A and its shifted form A^*:

$$A = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 2 & 3 & 0 \\ 0 & 0 & 2 & 4 & 6 \end{bmatrix},\ A^* = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 0 & 0 \\ 2 & 4 & 6 & 0 & 0 \end{bmatrix}$$

According to (13), the corresponding shifting matrix is:

$$S = \begin{bmatrix} 0 & -\frac{36}{43} & -\frac{36}{43} & \frac{80}{43} & \frac{67}{43} \\ -\frac{2}{3} & -\frac{25}{43} & -\frac{161}{129} & \frac{319}{258} & \frac{487}{258} \\ \frac{1}{3} & \frac{9}{86} & \frac{113}{258} & -\frac{17}{258} & \frac{25}{258} \\ \frac{1}{3} & \frac{34}{43} & \frac{145}{129} & -\frac{95}{258} & -\frac{179}{258} \\ 0 & \frac{9}{86} & \frac{9}{86} & \frac{23}{86} & \frac{37}{86} \end{bmatrix}$$

and it can be easily verified that $A^* = A \cdot S$. □

Obviously, the shifting operation alters the structure of a matrix. Therefore, even if the original matrix has full rank, the corresponding shifted matrix may not have full rank. For instance, in the previous Example 1 we have $\rho(A) = 3$ and $\rho(A^*) = 2$. However, in the case where both A and A^* have full rank we obtain the following result.

Corollary 1. *If $A \in \mathbb{R}^{m \times n}$, $m < n$, is a nonsingular upper trapezoidal matrix with rank $\rho(A) = m$ and $A^* \in \mathbb{R}^{m \times n}$ is the shifted matrix of A with rank $\rho(A^*) = m$, then there exists an invertible matrix $S \in \mathbb{R}^{n \times n}$ with rank $\rho(S) = n$, such that*

$$A^* = A \cdot S \;\Leftrightarrow\; A = A^* \cdot S^{-1} \tag{14}$$

where S^{-1} denotes the inverse of S.

The previous corollary can be proven by following the same steps as in the proof of Theorem 2. We only have to change appropriately the set of permutation matrices $J_i,\ i = 1, 2, \ldots, m$ to achieve the proper shifting, and compute the inverse or pseudo-inverse of A^*. Therefore, we conclude that the shifting of a nonsingular upper trapezoidal matrix is a reversible process, unless the shifted matrix is rank deficient.

Remark 2. The results from Theorem 2 and Corollary 1 can also be applied to a square upper triangular matrix provided that this matrix is invertible.

The relations (8) and (14) have a key role in the general algebraic representation of the ERES method, since a) in every iteration of the main procedure there is always a nonsingular upper trapezoidal matrix which is formed after the application of the ERE operations, and b) the process stops when a rank-deficient matrix occurs and shifting cannot be applied.

4. The general algebraic representation of the ERES method

ERES is an iterative matrix-based method where, until now, only the ERE operations (i.e. triangularization and reordering of rows) could be represented by a matrix $R \in \mathbb{R}^{m \times m}$. With the introduction of the representation of the shifting operation as a matrix product in Theorem 2 it is now possible to form an algebraic expression representing all the required transformations until a rank-1 matrix is reached. This representation provides a link between the initial basis matrix and the last matrix which gives the coefficients of the GCD. This algebraic relationship is described by the following theorem.

Theorem 3. *Given a set $\mathcal{P}_{m,n}$ of m real univariate polynomials of maximum degree $n \in \mathbb{N}$ and its basis matrix $P_m \in \mathbb{R}^{m \times (n+1)}$, the application of the ERES operations to P_m results in a matrix $G \in \mathbb{R}^{m \times (n+1)}$ with rank $\rho(G) = 1$, which satisfies the equation:*

$$G = R \cdot P_m \cdot S \tag{15}$$

where $R \in \mathbb{R}^{m \times m}$ and $S \in \mathbb{R}^{(n+1) \times (n+1)}$ represent the applied row transformations (ERE operations) and the application of the shifting operation, respectively. The GCD of $\mathcal{P}_{m,n}$ is then represented by

$$\gcd\{\mathcal{P}_{m,n}\} = \underline{e}_1 \cdot G \cdot \underline{e}_n(s) \tag{16}$$

where $\underline{e}_1 = [1, 0, \ldots, 0] \in \mathbb{R}^m$ and $\underline{e}_n(s) = [1, s, s^2, \ldots, s^n]^t$.

Proof. Given a set $\mathcal{P}_{m,n}$ of $m > 2$ polynomials and its basis matrix P_m, let $P^{(1)} := P_m$ be the initial matrix and $P^{(k)}$ is the processed matrix at the beginning of the k^{th} iteration, $k \in \mathbb{N}$. The superscript "(k)", $k = 1, 2, 3, \ldots$, will be used in all matrices to indicate the number of iteration of the main procedure.

The ERES operations are performed in the following order:

1. Construct the permutation matrix $J^{(1)} \in \mathbb{R}^{m\times m}$ which reorders the rows of the initial matrix such that the first row corresponds to the polynomial with the lowest degree in the set.
2. Apply the elementary row transformations (ERE operations) by using an appropriate lower triangular matrix $L^{(1)} \in \mathbb{R}^{m\times m}$.
3. Delete (or reorder) the zero rows by using an appropriate permutation matrix $Z^{(1)} \in \mathbb{R}^{r_1\times m}$, $r_1 \leq m$.
4. Apply the shifting operation by using an appropriate square matrix $S^{(1)} \in \mathbb{R}^{(n+1)\times(n+1)}$.

Therefore, after performing the above transformations, the resulting matrix is

$$P^{(2)} = Z^{(1)} \cdot L^{(1)} \cdot J^{(1)} \cdot P^{(1)} \cdot S^{(1)} \tag{17}$$

If we set $R^{(1)} = Z^{(1)} \cdot L^{(1)} \cdot J^{(1)}$, then it follows

$$P^{(2)} = R^{(1)} \cdot P^{(1)} \cdot S^{(1)} \tag{18}$$

The equation (18) represents the first complete iteration of the main procedure of the ERES method. The whole process terminates when a matrix with rank equal to 1 appears. This can be practically achieved in less than $n+1$ iterations. Therefore, after the k^{th} iteration we have

$$P^{(k+1)} = R^{(k)} \cdot P^{(k)} \cdot S^{(k)}, \quad k = 1, 2, \ldots \tag{19}$$

and, if the final number of iterations is $\ell \in \mathbb{N}$, then

$$P^{(\ell+1)} = R^{(\ell)} \cdots R^{(1)} \cdot P_m \cdot S^{(1)} \cdots S^{(\ell)} \;\Leftrightarrow$$

$$P^{(\ell+1)} = \tilde{R} \cdot P_m \cdot S \tag{20}$$

where we denote by

$$\tilde{R} = \prod_{k=1}^{\ell} R^{(k)} \;\text{ and }\; S = \prod_{k=1}^{\ell} S^{(k)} \tag{21}$$

Obviously, the matrices $P^{(k)}$ do not necessarily have the same dimensions as the initial matrix P_m due to the frequent deletion of the produced zero rows during the iterative main procedure of the method. However, for theoretical purposes we may preserve the original dimensions of the basis matrix. This can be easily achieved if we change the permutation matrix $Z^{(k)}$ so as to move the zero rows of $P^{(k)}$ to the bottom of the matrix instead of deleting them. Therefore, in this case $P^{(k)}$ can have the same dimensions as P_m, but we actually continue to work with a $r_k \times (n+1)$ submatrix of $P^{(k)}$ with a decreasing row dimension $r_k < m$. Since the last matrix $P^{(\ell+1)}$ has rank equal to 1, every row gives the coefficients of the GCD. But if we triangularize $P^{(\ell+1)}$ once more by using an appropriate matrix $L^{(\ell+1)}$, then the final matrix $G \in \mathbb{R}^{m\times(n+1)}$ contains the coefficients of the GCD in its first row and it has zeros elsewhere. Hence,

$$G = L^{(\ell+1)} \cdot P^{(\ell+1)} \;\text{ and }\; R = L^{(\ell+1)} \cdot \tilde{R} \tag{22}$$

and the main result in (15) derives from the combination of (20), (21), and (22). Then, if $\underline{e}_1 = [1, 0, \ldots, 0] \in \mathbb{R}^m$ and $\underline{e}_n(s) = [1, s, s^2, \ldots, s^n]^t$, the GCD is given by

$$\gcd\{\mathcal{P}_{m,n}\} = \underline{e}_1 \cdot R \cdot P_m \cdot S \cdot \underline{e}_n(s) = \underline{e}_1 \cdot G \cdot \underline{e}_n(s) \tag{23}$$

□

The next example demonstrates the application of the ERES method to a set of three polynomials.

Example 2. Consider the set of polynomials:

$$\mathcal{P}_{m,n} = \left\{ \begin{array}{lcl} p_1(s) & = & s^3 - 2s^2 - 11s + 12 \\ p_2(s) & = & 2s^3 - 11s^2 + 13s - 4 \\ p_3(s) & = & s^2 - s - 12 \end{array} \right\}, \quad m = 3,\ n = 3$$

with $\gcd\{\mathcal{P}_{m,n}\} = s - 4$. The initial basis matrix is:

$$P_m = \begin{bmatrix} 12 & -11 & -2 & 1 \\ -4 & 13 & -11 & 2 \\ -12 & -1 & 1 & 0 \end{bmatrix} \in \mathbb{R}^{3\times 4}, \quad \underline{e}_n(s) = \begin{bmatrix} 1 \\ s \\ s^2 \\ s^3 \end{bmatrix} \tag{24}$$

The iterative main procedure of the ERES method will start with the matrix P_m. After two iterations of the main procedure, the final matrix will have rank equal to 1 and its first row gives the vector of coefficients of the GCD. The matrix R, which represents all the necessary row transformations, and the matrix S, which represents all the shifting transformations, have the form:

$$R = \begin{bmatrix} \frac{5}{14} & \frac{9}{28} & \frac{1}{4} \\ -\frac{10}{7} & -\frac{9}{7} & 0 \\ 1 & 0 & 0 \end{bmatrix} \quad \text{and} \quad S = \begin{bmatrix} \frac{529687}{397579} & -\frac{120713}{397579} & \frac{551}{23387} & \frac{69}{4369} \\ \frac{528432}{397579} & -\frac{85273}{397579} & \frac{2204}{23387} & \frac{276}{4369} \\ \frac{523412}{397579} & \frac{56487}{397579} & \frac{8816}{23387} & \frac{1104}{4369} \\ \frac{503332}{397579} & \frac{623527}{397579} & \frac{35264}{23387} & \frac{4416}{4369} \end{bmatrix} \tag{25}$$

The computation of the shifting matrices during the iterations corresponds to (13). The final matrix is

$$G = \begin{bmatrix} -4 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \in \mathbb{R}^{3\times 4} \tag{26}$$

and it can be verified that:

$$G = R \cdot P_m \cdot S$$

If $\underline{e}_n(s) = [1, s, s^2, s^3]^t$ and $\underline{e}_1 = [1, 0, 0, 0]$, then the GCD of the set $\mathcal{P}_{m,n}$ can be expressed as:

$$\gcd\{\mathcal{P}_{m,n}\} = \underline{e}_1 \cdot R \cdot P_m \cdot S \cdot \underline{e}_n(s) = s - 4 \tag{27}$$

□

5. Analysis of the numerical stability of the ERES method

Based on the relation (15) we can now develop a detailed analysis of the numerical stability of the method for all the performed iterations of its main procedure.

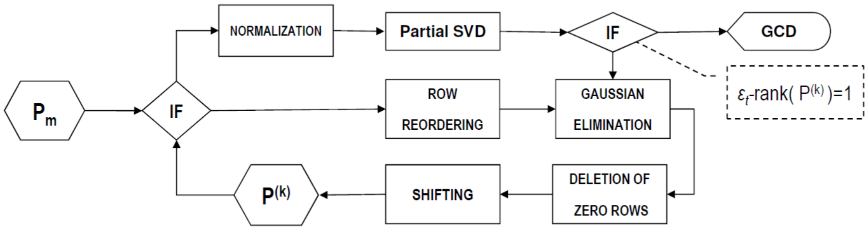

Figure 1: The ERES algorithm

5.1. The basics of the ERES algorithm

The development of an effective numerical algorithm for the ERES method, requires [21]:

a) to find a robust numerical procedure for the application of the ERE operations,

b) to develop a proper termination criterion for the algorithm, and finally

c) to find a reliable way to extract the coefficients of the GCD from the last rank-1 matrix.

These requirements are the most essential parts of the ERES algorithm (Fig.1) and in the following we will consider them in the context of a numerical implementation in a floating-point computational environment. Having a basis matrix of a set of polynomials, the ERES algorithm involves row addition or row multiplication, row reordering, elimination of zero rows and shifting. We refer to this process as the *main procedure* of the ERES algorithm. The most reliable and stable numerical method for applying elementary row operations is the *Gaussian elimination with partial pivoting* (GEPP) [24, 25]. Hence, an upper triangular or trapezoidal form of the basis matrix is computed. The shifting operation is merely a permutation of the leading consecutive zero elements in a row.

The algorithm's termination criterion relies on the proper detection of the final unity rank matrix which is based on the numerical computation of the singular values of an associated normalized matrix obtained at the end of each iteration of the main procedure. We shall refer to it as the *Rank-1 procedure* of the ERES algorithm. This property is detected numerically according to the inequality [21]:

$$|\sigma_1 - \sqrt{\mu}| \leq \varepsilon_t \text{ and } \sigma_i \leq \varepsilon_t, \ i = 2, 3, \dots, \mu \tag{28}$$

where σ_i are the singular values of a normalized matrix with $\mu < m$ rows, which is formed at the end of the main procedure, and σ_1 corresponds to the maximum singular value. The tolerance ε_t is referred to as the *termination accuracy* of the ERES algorithm in finite precision computations.

When a matrix P with ε_t-rank=1 is achieved, the vector of the coefficients of the GCD is given by the first row of the matrix:

$$G_1 = \sigma_1 \cdot \underline{u} \cdot \underline{w}^t \tag{29}$$

where $\underline{u}$ and $\underline{w}$ are the first columns of the orthogonal matrices U and W of the singular value decomposition $P = U \cdot \Sigma \cdot W^t$, respectively [21].

5.2. Estimation of the total numerical error of the ERES method

Let us denote by $P^{(k)} = [p_{ij}^{(k)}] \in \mathbb{R}^{r_k \times (n+1)}$ the matrix to be processed at the k^{th} iteration of the main procedure of the ERES algorithm with $r_k \leq m$ and $k \in \mathbb{N}$. The superscript "(k)" will be used in all matrices to indicate the number of iteration of the main procedure, and $P^{(1)} := P_m$. If we denote by $d > 0$ the degree of the GCD, the constant application of the shifting operation gradually zeros the last $n - d$ columns of P_m, and therefore we will denote by n_k the number of the first consecutive nonzero columns of $P^{(k)}$. Clearly, $n_k \leq n + 1$, and hence we may consider $P^{(k)}$ as an $r_k \times n_k$ matrix. In the following, we shall consider the numerical error for each individual step of the main procedure of the ERES algorithm and we will conclude with the total numerical error of the method. We measure this error by using the infinity matrix norm $\| \cdot \|_\infty$ which is invariable under the row-reordering and shifting transformations.

Starting the main procedure, we must reorder the rows of $P^{(k)}$ such that the first row corresponds to the least degree polynomial. This is a basic step of the ERES method, but, in order to prevent a further change during the process of GEPP, it is required to scale the elements of the matrix, such that the first element $p_{11}^{(k)}$ of the first column can be larger in magnitude than the other elements of the first column. This normalization can be achieved if we multiply $P^{(k)}$ by an appropriate diagonal matrix $N_1 \in \mathbb{R}^{r_k \times r_k}$ with $\|N_1\|_\infty = 1$, [22], such that

$$\tilde{P}^{(k)} = N_1 \, P^{(k)} + E_1 \tag{30}$$

where E_1 is the error matrix and

$$\|E_1\|_\infty \leq n_k \, \mathbf{u} \, \|P^{(k)}\|_\infty \tag{31}$$

where $\mathbf{u}$ is the machine precision ($\mathbf{u} = \frac{1}{2} b^{-t} = 2^{-53}$ in binary 64 bits arithmetic, known as "double precision"). However, this normalization is not always necessary to be performed and in practise this error is negligible compared to the error produced from the GEPP process.

A further normalization of $P^{(k)}$ can be added so that every element of $P^{(k)}$ is bounded by unity. This normalization can be written as [24]:

$$\widetilde{P}^{(k)} = N^{(k)} \, P^{(k)} + E_N^{(k)} \tag{32}$$

where $N^{(k)}$ is a diagonal $r_k \times r_k$ matrix of the form:

$$N^{(k)} = \operatorname{diag}\left\{ \|p_{1j}^{(k)}\|_2^{-1}, \|p_{2j}^{(k)}\|_2^{-1}, \ldots, \|p_{rj}^{(k)}\|_2^{-1} \right\} \text{ for } j = 1, 2, \ldots n_k$$

and $E_N^{(k)}$ is the error matrix with

$$\|E_N^{(k)}\|_\infty \leq n_k \, \mathbf{u} \, \|P^{(k)}\|_\infty \tag{33}$$

Consequently, $\|\widetilde{P}^{(k)}\|_\infty \leq n_k$.

The backward error analysis of the Gaussian elimination with partial pivoting [26] shows that the computed upper and lower triangular matrices $L^{(k)}$ and $U^{(k)}$ satisfy:

$$L^{(k)} \cdot U^{(k)} = \widetilde{P}^{(k)} + E_G^{(k)} \tag{34}$$

$$\|E_G^{(k)}\|_\infty \leq n_k^2 \, \rho_k \, \mathbf{u} \, \|\widetilde{P}^{(k)}\|_\infty \tag{35}$$

where $E_G^{(k)}$ is the error matrix and generally, $\|\widetilde{P}^{(k)}\|_\infty \leq \|P^{(k)}\|_\infty$. The term ρ_k denotes the *growth factor* [24], which is $\rho_k \leq 2^{n_k - 1}$ for GEPP, but in practice this bound is not attainable [26]. The upper triangular matrix $U^{(k)}$ will eventually give the next matrix $P^{(k+1)}$ after the deletion of its zero rows and shifting:

$$U^{(k)} = {L^{(k)}}^{-1} \left(\widetilde{P}^{(k)} + E_G^{(k)} \right) \tag{36}$$

and

$$P^{(k+1)} = Z^{(k)} \cdot U^{(k)} \cdot S^{(k)} \tag{37}$$

Therefore, at the end of the k^{th} iteration of the main procedure we have:

$$P^{(k+1)} = Z^{(k)} \cdot {L^{(k)}}^{-1} \left(\left(N^{(k)} \left(N_1 \cdot J^{(k)} \cdot P^{(k)} \right) + E_N^{(k)} \right) + E_G^{(k)} \right) S^{(k)} \tag{38}$$

Then, we may set

$$R^{(k)} = Z^{(k)} \cdot {L^{(k)}}^{-1} \cdot N^{(k)} \cdot N_1 \cdot J^{(k)} \tag{39}$$

and the error matrix for the k^{th} iteration is

$$E^{(k)} = Z^{(k)} \cdot {L^{(k)}}^{-1} \left(E_N^{(k)} + E_G^{(k)} \right) S^{(k)} \tag{40}$$

The reordering of rows, the deletion of zero rows, and the shifting are error-free transformations, since they do not alter the values of the data. Especially for the shifting operation, there is no need to compute the shifting matrices $S^{(k)}$. We only use them in order to connect the matrices $P^{(k)}$ which are generated in every iteration of the main procedure. Thus, for practical reasons we may set $\|S^{(k)}\|_\infty = 1$. According to the form of the matrices in (40) it is $\|Z^{(k)}\|_\infty = 1$, and for normalized matrices we have $\|{L^{(k)}}^{-1}\|_\infty \leq n_k$ [26]. Hence, if we combine the relations (33), (35), and (40) we conclude with the result in the next lemma, which describes the numerical error $E^{(k)}$ produced in every iteration of the main procedure of the ERES algorithm.

Lemma 1. *The matrix $P^{(k+1)}$, $k \in \mathbb{N}$, which is produced after the numerical processing of the matrix $P^{(k)} \in \mathbb{R}^{r_k \times n_k}$ during the main procedure of the ERES algorithm, satisfies the equation:*

$$P^{(k+1)} = R^{(k)} \cdot P^{(k)} \cdot S^{(k)} + E^{(k)} \tag{41}$$

with

$$\|E^{(k)}\|_\infty \leq \left(n_k^3 \, \rho_k + n_k^2 \right) \mathbf{u} \, \|P^{(k)}\|_\infty \tag{42}$$

where $R^{(k)}$ denotes the matrix for the combined ERE operations and $S^{(k)}$ denotes the matrix for the shifting transformation during the k^{th} iteration of the main procedure.

If we denote by ℓ the total number of iterations of the main procedure of the ERES algorithm, then the total numerical error E for all the performed iterations is

$$E = \sum_{k=1}^{\ell} E^{(k)} \tag{43}$$

with

$$\|E\|_\infty \leq \left(\sum_{k=1}^{\ell} \left(n_k^3 \, \rho_k + n_k^2 \right) \right) \mathbf{u} \, \|P_m\|_\infty \tag{44}$$

However, the error in (44) depends on the column dimension n_k of $P^{(k)}$ which decreases in a non-uniform way. But, since $n_k \leq n+1$ for all $k = 1, 2, \ldots, \ell$, we can establish a higher (theoretical) bound which characterizes the overall numerical stability of the ERES algorithm in finite precision arithmetic.

Theorem 4 (Numerical stability of the ERES method). *Given a set of m real univariate polynomials of maximum degree $n \in \mathbb{N}$, $P_m \in \mathbb{R}^{m \times (n+1)}$ the basis matrix, and $\varepsilon_t > 0$ a small tolerance, the iterative application of the ERES operations to $P^{(1)} := P_m$ using numerical finite precision computations results in a matrix $P^{(\ell+1)} \in \mathbb{R}^{r_{\ell+1} \times (n+1)}$ with numerical ε-rank=1 which satisfies the equation:*

$$P^{(\ell+1)} = R \cdot P_m \cdot S + E \tag{45}$$

where $R \in \mathbb{R}^{r_{\ell+1} \times m}$ and $S \in \mathbb{R}^{(n+1) \times (n+1)}$ represent the combined row transformations (ERE operations) and the application of the shifting operation, respectively. The matrix E provides the total numerical error, such that

$$\|E\|_\infty \leq \left(\ell \, (n+1)^3 \, \rho + O(n^2) \right) \, \mathbf{u} \, \|P_m\|_\infty \tag{46}$$

where ℓ denotes the total number of applications of the ERES operations to the basis matrix P_m.

In (45) the matrix R is defined as the matrix product of all $R^{(k)}$ as given in (39), and S is defined as the matrix product of all $S^{(k)}$ for $k = 1, 2, \ldots, \ell$. In (46) the term ρ denotes the growth factor which corresponds to the first Gaussian elimination for the basis matrix P_m, and $O(n^2)$ denotes a polynomial function of n with maximum degree 2. The proof of the above theorem follows from Lemma 1 and the preceding results.

The singular value decomposition (SVD) during the Rank-1 procedure is applied to a copy of the matrix $P^{(k)}$ only when it is required [21]. Thus, the processing of $P^{(k)}$ in the Rank-1 procedure does not numerically affect the data during the iterations the main procedure [23]. The preliminary stage in the SVD algorithm is the bidiagonal reduction of $P^{(k)}$ and in most bidiagonal reduction methods the error is expressed in the following form [24, 25]:

$$P^{(k)} + \delta P^{(k)} = U \, B \, V^t \tag{47}$$

$$\|\delta P^{(k)}\|_2 \leq f(r_k, n_k) \, \mathbf{u} \, \|P^{(k)}\|_2 \tag{48}$$

where B is bidiagonal, U and V are orthogonal, and $f(r_k, n_k)$ is a modestly growing function of the dimensions of $P^{(k)}$ [24, 25], where $r_k \leq m$ and $n_k \leq n+1$. The error (48) is not accumulated during the iterations of the main procedure of the ERES algorithm, but a small error of the form (48) for $r_k = r_{\ell+1}$ and $n_k = d+1$ must be taken into account for the final solution. Therefore, the total numerical error mainly comes from the application of the processes of normalization and Gaussian elimination during the iterative main procedure which is given in (46).

Method	Rel. Error	Time (msec)
MPGCD	$1.4367948\,10^{-11}$	78
QuasiGCD	$9.1428733\,10^{-13}$	62
SubGCD	$1.0736840\,10^{-14}$	15
QRGCD	$1.0123822\,10^{-15}$	93
ERES	$8.7271766\,10^{-16}$	31

Table 1: Comparison of GCD methods (Example 3)

5.3. Remarks on the numerical performance of the ERES algorithm

The main advantages of the ERES algorithm are:

a) the processing of all the polynomials of a given set <u>simultaneously</u> by creating an initial basis matrix of the least possible dimensions, and

b) its ability to constantly reduce the dimensions of the initial matrix and hence reduce the amount of data during the processing, which results in fast data processing and lower usage of computer memory.

Tests on sets of more than two polynomials have showed that the numerical ERES algorithm behaves well producing sufficiently accurate results [22, 27, 28].

Example 3. Consider the set of polynomials:

$$\mathcal{P}_{m,n} = \left\{ \begin{array}{lcl} p_1(s) & = & 0.87\,s^4 - 31.14\,s^3 + 108.21\,s^2 - 55.38\,s - 32.01 \\ p_2(s) & = & -0.65\,s^4 + 22.76\,s^3 - 63.74\,s^2 + 12.87\,s - 32.98 \\ p_3(s) & = & -0.16\,s^3 + 6.49\,s^2 - 46.67\,s + 86.33 \\ p_4(s) & = & 0.30\,s^3 - 9.96\,s^2 + 10.20\,s + 52.38 \end{array} \right\}$$

with $m = 4$, $n = 4$ and exact GCD $g(s) = s^2 - 35\,s + 97$.

In this example, the ERES method, the Matrix Pencil method (MPGCD) [29], the subspace method (SubGCD) [30], the quasi-GCD method (QuasiGCD) [5], and the QRGCD method [9] are used in order to compute the GCD of the given set in a typical 16-digits arithmetic system (machine precision $\mathbf{u} \approx 2.2\,10^{-16}$). We evaluate the results by measuring the relative error between the exact and the computed solution, which is given by $Rel = \frac{\|\underline{v}-\underline{g}\|_2}{\|\underline{g}\|_2}$, where $\underline{v}$, $\underline{g}$ are the coefficient vectors of the provided solution $v(s)$ and the exact GCD $g(s)$ respectively. The required time of processing in milliseconds is also provided and these results are presented in Table 1. The solution given by ERES has the smallest relative error found and it was obtained in relative short time. □

Considering the previous Example 3, it is important to stress that QuasiGCD and QRGCD algorithms[1] are designed to work with two polynomials. In the case of many polynomials they work iteratively with two polynomials at a time, but they tend to fail, especially in the case of large sets of polynomials. Conversely, ERES, MPGCD, and SubGCD are matrix-based algorithms which are designed to work with all the polynomials simultaneously, either in a direct or iterative way, and produce better results.

[1] QuasiGCD and QRGCD are parts of the SNAP package in MAPLE 16 (Maplesoft, Waterloo Maple Inc.).

Set	Method	Tolerance	Rel. Error	Time(msec)
(A)	ERES	10^{-16}	$5.0398803\,10^{-16}$	125
m=10	SubGCD	10^{-16}	$4.3369269\,10^{-15}$	94
n=10	MPGCD	10^{-8}	$4.0010207\,10^{-10}$	202
d=3	QRGCD	10^{-15}	$1.3419339\,10^{-15}$	109
	QuasiGCD	10^{-15}	$4.0030939\,10^{-6}$	94
(B)	ERES	10^{-16}	$4.5948046\,10^{-16}$	8549
m=20	SubGCD	10^{-16}	$1.2802986\,10^{-13}$	4181
n=40	MPGCD	FAIL	FAIL	FAIL
d=10	QRGCD	10^{-10}	$2.1016595\,10^{-10}$	4024
	QuasiGCD	FAIL	FAIL	FAIL
(C)	ERES	10^{-16}	$2.4916347\,10^{-16}$	343
m=50	SubGCD	10^{-16}	$2.2638888\,10^{-14}$	484
n=20	MPGCD	10^{-5}	$9.9727246\,10^{-1}$	827
d=5	QRGCD	10^{-12}	$7.3988778\,10^{-13}$	750
	QuasiGCD	FAIL	FAIL	FAIL

m = number of polynomials in the set, n = maximum degree of polynomials,
d = degree of the exact GCD

Table 2: Comparison of GCD methods for random sets of polynomials

In Table 2 we present a sample of the results given by the above algorithms for the computation of the GCD of randomly selected sets of many polynomials. Generally, the ERES and SubGCD algorithms succeeded in producing a solution with very small relative error close enough to machine precision ($\mathbf{u} \approx 2.2\,10^{-16}$). QRGCD algorithm also succeeded in producing solutions with the same degree as the exact GCD, but for higher values of its tolerance ($eps > 10^{-16}$) and consequently larger relative error. The other two methods, MPGCD and QuasiGCD, failed or produced a solution with smaller degree than the exact GCD in the most cases of large sets of polynomials. More tests and comparison with other methods can be found in [28].

Regarding the total numerical error of the ERES method, it is obvious from (46) that it depends on how many iterations ℓ of the main procedure of the algorithm are performed. Practically, ℓ is much less than the maximum polynomial degree n and it strongly depends on the linear dependence of the coefficient vectors of the polynomials, i.e. the rank of the initial basis matrix. For instance, for large sets of polynomials of high degree if $\rho(P_m) << n$, then we expect a number of iterations close to n. Conversely, if $\rho(P_m) = n + 1 - d$, where d denotes the degree of the GCD, then the GCD can be computed in just two iterations. The following example demonstrates this case in a general form.

Example 4. Consider an arbitrary set of polynomials $\mathcal{P}_{m,n}$, $m = 8$, $n = 4$ and $d = 1$. Let $P_m \in \mathbb{R}^{m\times(n+1)}$ be the initial basis matrix in arbitrary form, where its non-zero elements are symbolized with "$*$" and assume that $\rho(P_m) = n + 1 - d = 4$. Then, by using the ERES method we get:

Iteration 1:

$$\begin{bmatrix} * & * & * & * & * \\ * & * & * & * & * \\ * & * & * & * & * \\ * & * & * & * & * \\ * & * & * & * & * \\ * & * & * & * & * \\ * & * & * & * & * \\ * & * & * & * & * \end{bmatrix} \xrightarrow{\substack{\text{Gaussian}\\ \text{elimination}}} \begin{bmatrix} * & * & * & * & * \\ 0 & * & * & * & * \\ 0 & 0 & * & * & * \\ 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \xrightarrow{\substack{\text{Zero row deletion}\\ \text{and shifting}}} \begin{bmatrix} * & * & * & * & * \\ * & * & * & * & 0 \\ * & * & * & 0 & 0 \\ * & * & 0 & 0 & 0 \end{bmatrix}$$

Iteration 2:

$$\begin{bmatrix} * & * & 0 & 0 & 0 \\ * & * & * & 0 & 0 \\ * & * & * & * & 0 \\ * & * & * & * & * \end{bmatrix} \xrightarrow{\substack{\text{Gaussian}\\ \text{elimination}}} \begin{bmatrix} * & * & 0 & 0 & 0 \\ 0 & * & * & 0 & 0 \\ 0 & 0 & * & * & 0 \\ 0 & 0 & 0 & * & * \end{bmatrix} \xrightarrow{\text{Shifting}} \begin{bmatrix} * & * & 0 & 0 & 0 \\ * & * & 0 & 0 & 0 \\ * & * & 0 & 0 & 0 \\ * & * & 0 & 0 & 0 \end{bmatrix}$$

The last matrix has column dimension equal to $d+1$ and, provided that it has rank 1, every row gives the coefficients of the GCD with degree $d = 1$. □

However, there are cases where the iterative nature of the ERES method acts as disadvantage, especially when the number of iterations is high and inexact data are present. GEPP is a quite stable numerical process, but although pivoting keeps the multipliers bounded by unity, the elements in the reduced matrices still can grow arbitrarily [24, 26] during the iterations. Therefore, in fixed-precision arithmetic the error in (44) may become prohibitively large. This problem motivated the search for a new kind of implementation for the ERES method which improves its performance and reliability and made it suitable for computing an approximate GCD for sets of polynomials with inaccurate data. A major step towards this direction is the usage of different types of arithmetic, such as rational and numeric (variable floating-point) arithmetic. The benefits from the mixture of rational and numeric computations, known as *hybrid computations*, are significant and thus hybrid computations are widespread nowadays. The development of the hybrid implementation of the ERES algorithm optimized for the approximate GCD problem has been described in [23], and it is referred to as the *Hybrid ERES algorithm* (H-ERES). More information about the hybridization of the ERES method and comparison with other methods can be found in [23, 28].

6. Conclusions

In this paper, the fundamental theoretical and numerical properties of the ERES method for computing the greatest common divisor of sets of many polynomials were presented and analysed. The general algebraic representation of the method is presented in Theorem 3 and requires the shifting operation to be written as a matrix product just like the elementary row operations. In Theorem 2 it is now proven that the shifting operation applied to upper trapezoidal matrices with full rank can be represented as a simple matrix product. The main problem in this study was to analyse the overall numerical stability of the ERES method. In Theorem 4, a total numerical error bound is now established for all the iterations of the ERES algorithm which indicates that, under certain conditions, the method is numerically stable for large sets of polynomials. These results are demonstrated through numerical examples. The accuracy of the solutions given by the ERES algorithm reveals that ERES is an efficient method for the computation of the greatest common divisor of sets of many polynomials compared to other GCD methods.

References

[1] T. L. Heath, The Thirteen Books of Euclid's Elements, Dover Publications, 2nd edn., 1956.

[2] W. Blankiship, A new version of Euclid's Algorithm, American Mathematics Monthly 70 (1963) 742–744.

[3] W. S. Brown, On Euclid's algorithm and the computation of polynomials Greatest Common Divisors, Journal of the Association for Computer Machinery 18 (4) (1971) 478–504.

[4] I. S. Pace, S. Barnett, Comparison of algorithms for calculation of g.c.d of polynomials, Int. J. Control 4 (2) (1973) 211–216.

[5] A. Schöenhage, Quasi-GCD computations, J. Complexity 1 (1985) 118–137.

[6] M. T. Noda, T. Sasaki, Approximate GCD and its applications to ill-conditioned algebraic equations, J. Comp. Appl. Math. 38 (1991) 335–351.

[7] N. Karcanias, C. Giannakopoulos, M. Hubbard, Almost zeros of a set of polynomials of R[s], Int. J. Control 38 (1983) 1213–1238.

[8] P. Chin, R. M. Corless, G. F. Corliss, Optimization Strategies for the Approximate GCD Problem, in: Proc. ISSAC'98, Rostock, Germany, 228–235, 1998.

[9] R. M. Corless, S. M. Watt, L. Zhi, QR Factoring to compute the GCD of Univariate Approximate Polynomials, IEEE Transactions on Signal Processing 52 (12) (2004) 3394–3402.

[10] I. Z. Emiris, A. Galligo, H. Lombardi, Certified approximate univariate GCDs, J. Pure and Applied Algebra 117 & 118 (1997) 229–251.

[11] N. Karmarkar, Y. N. Lakshman, On approximate GCDs of univariate polynomials, J. Symbolic Computation 26 (6) (1998) 653–666.

[12] V. Y. Pan, Computation of Approximate Polynomial GCDs and an Extension, Information and Computation 167 (2001) 71–85.

[13] D. Rupprecht, An algorithm for computing certified approximate GCD of n univariate polynomials, J. Pure and Applied Algebra 139 (1999) 255–284.

[14] Z. Zeng, A method computing multiple roots of inexact polynomials, Mathematics of Computation 74 (2005) 869–903.

[15] D. A. Bini, P. Boito, Structured Matrix-Based Methods for Polynomial ϵ-gcd:Analysis and Comparison, in: Proc. ISSAC'07, Waterloo, Ontario, Canada, 9–16, 2007.

[16] J. R. Winkler, X. Lao, The calculation of the degree of an approximate greatest common divisor of two polynomials, J. Comp. Appl. Math. 235 (2011) 1587–1603.

[17] S. Barnett, Greatest common divisor of several polynomials, in: Proc. Cambridge Philos. Soc., 263–268, 1971.

[18] S. Barnett, Greatest common divisor from generalized Sylvester matrices, in: Proc. Cambridge Philos. Soc., vol. 8, 271–279, 1980.

[19] L. Gonzales-Vega, An elementary proof of Barnett's theorem about the greatest common divisor of several univariate polynomials, Linear Algebra and its Applications 247 (1996) 185–202.

[20] N. Karcanias, Invariance properties and characterisation of the greatest common divisor of a set of polynomials, Int. J. Control 46 (1987) 1751–1760.

[21] M. Mitrouli, N. Karcanias, Computation of the GCD of polynomials using Gaussian transformation and shifting, Int. J. Control 58 (1993) 211–228.

[22] M. Mitrouli, N. Karcanias, C. Koukouvinos, Further numerical aspects of the ERES algorithm for the computation of the greatest common divisor of polynomials and comparison with other existing methodologies, Utilitas Mathematica 50 (1996) 65–84.

[23] D. Christou, N. Karcanias, M.Mitrouli, The ERES method for computing the approximate GCD of several polynomials, Applied Numerical Mathematics 60 (2010) 94–114.

[24] B. N. Datta, Numerical Linear Algebra and Applications, SIAM, Philadelphia, USA, 2nd edn., 2010.

[25] G. H. Golub, C. F. Van Loan, Matrix Computations, The John Hopkins University Press, Baltimore, London, 2nd edn., 1989.

[26] J. H. Wilkinson, Rounding Errors in Algebraic Processes, Her Majesty's Stationary Office, London, 1963.

[27] M. Mitrouli, N. Karcanias, C. Koukouvinos, Numerical performance of the matrix pencil algorithm computing the greatest common divisor of polynomials and comparison with other matrix-based methodologies, J. Comp. Appl. Math. 76 (1996) 89–112.

[28] D. Christou, N. Karcanias, M. Mitrouli, D. Triantafyllou, Numerical and symbolical methods for the GCD of several polynomials, in: Numerical Linear Algebra in Signals, Systems and Control, vol. 80 of *Lecture Notes in Electrical Engineering*, Springer, 123–144, 2011.

[29] N. Karcanias, M. Mitrouli, A Matrix Pencil Based Numerical Method for the Computation of the GCD of Polynomials, IEEE Trans. Autom. Cont. 39 (1994) 977–981.

[30] W. Qui, Y. Hua, K. Abed-Meraim, A subspace method for the computation of the GCD of polynomials, Automatica 33 (4) (1997) 255–284.

***Revision Notes**

Revision of the paper

Matrix Representation of the Shifting Operation and Numerical Properties of the ERES Method for Computing the Greatest Common Divisor of Sets of Many Polynomials

by D. Christou, N. Karcanias and M. Mitrouli

Submitted to the Journal of Computational and Applied Mathematics

List of changes

The following changes have been applied to the paper according to the referee's report:

Reviewer #1

Reviewer's comment:

> *"the manuscript is quite good but it is long and my advice is to decrease the text."*

Authors' answer:
The revised version of the paper is now 6 pages shorter than its previous version.

Reviewer #2:

Reviewers' comments:

> *It is a nice paper.*
> *But there are several issues to be addressed:*
>
> *1. The authors do not mention the other methods to compute GCD ? They should provide state-of-art methods to compare advantages and disadvantages*

Authors' answer:
New paragraphs have been added in the introduction with the classification of GCD methods and additional citation to other GCD methods. Advantages and disadvantages are also discussed.

> *2. "ERES method to handle large sets polynomials and to invoke an efficient termination criterion", there is no numerical example to show the efficiency of the method*

Authors' answer:
We provide in Table 2 the results from examples with large sets of polynomials and compare them with other four GCD algorithms which are available by their developers or included in commercial software packages, such as Maple. ERES produces solutions with less numerical error than the other methods due to its algorithm structure and the SVD-based termination criterion which is described in section 5.

> *3. The paper is too long, they should present in a concise manner*

Authors' answer:
The paper is 6 pages shorter than its previous version. The entire Section 5 in the previous version has now been removed and we focus only on the basic numerical properties of the method. We intend to include the removed section in future publications considering the LCM problem. The other sections were reorganized and presented concisely.

4. No numerical comparisons with the other methods in terms efficiency and stability

Authors' answer:
We provide examples where the ERES method is compared with four other methods and the results are given in Tables 1 and 2. Advantages and disadvantages are also discussed. The comparison refers to the relative error between the exact and the computed GCD, which characterizes the stability of the method. The required time of processing is also provided. These tests are implemented in Maple and the spreadsheets are available by the corresponding author. Additional references to papers where the ERES method has been tested and compared with other GCD methods is also given.

5. There are some JCAM papers in this topic, they should cite them.

Authors' answer:
Three JCAM papers have been cited [6], [16] and [27].