Structured Matrix Methods Computing the Greatest Common Divisor of Polynomials

Abstract: This paper revisits the Bézout, Sylvester, and power-basis matrix representations of the greatest common divisor (GCD) of sets of several polynomials. Furthermore, the present work introduces the application of the QR decomposition with column pivoting to a Bézout matrix achieving the computation of the degree and the coefficients of the GCD through the range of the Bézout matrix. A comparison in terms of computational complexity and numerical efficiency of the Bézout-QR, Sylvester-QR, and subspace-SVD methods for the computation of the GCD of sets of several polynomials with real coefficients is provided. Useful remarks about the performance of the methods based on computational simulations of sets of several polynomials are also presented.

Keywords: Sylvester matrix; Bézout matrix; QR decomposition, Singular value decomposition

1 Introduction

The greatest common divisor (GCD) of a polynomial set is proven to be very important to many applications in applied mathematics and engineering. Several methods have been proposed for the computation of the GCD of sets of polynomials. Most of them are based on the Euclidean algorithm. They are designed to process two polynomials at a time [5] and can be applied iteratively when a set of more than two polynomials is considered [18, 21]. Conversely, there exist efficient matrix-based methods which can compute the degree and the coefficients of the GCD by applying specific transformations to a matrix formed directly from the coefficients of the polynomials of the entire given set [2, 16, 19].

The greatest common divisor has a significant role in Control Theory, Network Theory, signal and image processing [14, 24] and in several other areas of mathematics. A number of important invariants for Linear Systems rely on the notion of the greatest common divisor of many polynomials. In fact, it is instrumental in defining system notions such as zeros, decoupling zeros, zeros at infinity or notions of minimality of system representations. Conversely, Systems and Control methods provide concepts and tools, which enable the development of new computational procedures for GCD [17]. A major challenge for the control theoretic applications of the GCD is that frequently we have to deal with a very large number of polynomials. It is this requirement that makes the pairwise type approaches for GCD not suitable for such applications [25]. However, matrix-based methods tend to have better performance and quite good numerical stability, especially in the case of large sets of polynomials, because they use the entire set of polynomials.

Barnett’s GCD method [2] is a well known method for computing the GCD of several polynomials through the construction of the companion matrix $C_A$ of a properly selected polynomial from the given set and the
decomposition of a special controllability matrix. Considering the computation of the GCD of more than two polynomials without restricting to pairwise computations, Barnett’s theorems provided for the first time an alternative to standard approaches based on the Euclidean algorithm, since the GCD can be found in a single step by solving a system of linear equations. Two proofs are proposed in [2] for the result concerning the degree of the GCD, where the first uses the Jordan form of $C_A$ and the second is based on a theorem introduced in [1] which refers to the degree of the greatest common divisor of two invariant factors for two regular polynomial matrices. In [13] a more elementary proof is proposed and generalizes Barnett’s results to the case where the polynomials considered have their coefficients in an integral domain. However, Barnett’s method tends to be computationally ineffective for large sets of polynomials of high degree. An earlier comparison with other methods can be found in [22].

A variation of Barnett’s method through Bezoutians, found in [9], involves Bézout-like matrices and singular value decomposition, and suggests a very compact way of parametrising and representing the GCD of several univariate polynomials. Another approach using Sylvester-like matrices can be found in [3] which provides similar results. Structured matrices, such as Sylvester, Bézout, and Cauchy-like, were also used for the computation of the GCD of polynomials in Boito’s thesis [6].

The present work introduces the application of the QR decomposition with column pivoting (QRCP) to a Bézout matrix, achieving the computation of the degree and the coefficients of the GCD through the range of the Bézout matrix. This method provides the means for a more efficient implementation of the classical Bézout-QR method [2, 9] with less computational complexity and without compromising accuracy, and it enriches the existing framework for the computation of the GCD of several polynomials using structured matrices. The classical GCD representations through structured matrices are revisited and their computational complexity is theoretically analyzed and compared. Demonstrative examples explaining the application of each method are given. The paper is structured as follows.

In Section 2, we propose the use of the rank revealing QR with column pivoting for the computation of the GCD of polynomials through Bézout-like matrices which improves the numerical behavior of the existing Bézout-QR algorithms. Also, we revisit the representation of the GCD of sets of polynomials through Sylvester-like and power-basis matrices to highlight the importance of the structure in the computational complexity of a method. Furthermore, we discuss the use of the bowe-basis method for multivariate polynomials through rational implementation. In Section 3, we refer to the implementation of the GCD computation through matrix factorization. We study the behavior of the proposed algorithms with respect to computational complexity and we demonstrate the required steps through analytical examples. In Section 4, we present numerical examples and compare the computational performance of the methods through computational simulations measuring the required processing time and the relative error when the exact solution is known. Finally, in Section 5, we discuss the conclusions of the current study.

2 Representation of the GCD of a set of several polynomials

In this section we introduce the application of the rank revealing QR with column pivoting applied to Bézout matrices which results in the computation the degree and the coefficients of the GCD of polynomials with less floating-point operations, especially when the rank deficiency of the Bézout matrix is high. We also describe the Sylvester and power-basis matrix representations of a set of several polynomials and their corresponding GCD.

2.1 Representation of the GCD through Bézout matrices

A Bézout matrix is a special square matrix associated with two polynomials, introduced by Sylvester (1853) and Cayley (1857) and named after Étienne Bézout (1730 – 1783).
Definition 1. Let \( f(s) \) and \( g(s) \) two polynomials in one variable such that
\[
\begin{align*}
f(s) &= \sum_{l=0}^{n} u_l s^l = u_n s^n + u_{n-1} s^{n-1} + \ldots + u_2 s^2 + u_1 s + u_0 \\
g(s) &= \sum_{l=0}^{p} v_l x^l = v_p x^p + v_{p-1} x^{p-1} + \ldots + v_2 x^2 + v_1 x + v_0
\end{align*}
\]
with \( \deg(f(s)) = n \) and \( \deg(g(s)) = p \), where \( n \geq p \) and \( u_n, v_p \neq 0 \). Then, the Bézout matrix associated with the polynomials \( f(s) \) and \( g(s) \), denoted by \( B(f, g) \) or \( \text{Bez}(f(s), g(s)) \), is an \( n \times n \) symmetric matrix which is constructed from the coefficients of the polynomials as follows:
\[
B \triangleq B(f, g) = [b_{i,j}]_{i,j=1,...,n} = \begin{bmatrix}
    u_1 & \cdots & u_n \\
    \vdots & \ddots & \vdots \\
    u_n & 0 \\
\end{bmatrix} \begin{bmatrix}
    v_0 & \cdots & v_{n-1} \\
    0 & \ddots & 0 \\
    v_n & 0 \\
\end{bmatrix} - \begin{bmatrix}
    v_1 & \cdots & v_n \\
    \vdots & \ddots & \vdots \\
    0 & \ddots & 0 \\
\end{bmatrix} \begin{bmatrix}
    u_0 & \cdots & u_{n-1} \\
    \vdots & \ddots & \vdots \\
    0 & \ddots & 0 \\
\end{bmatrix}
\]
(1)

More specifically, the elements \( b_{i,j} \) of the Bézout matrix are given by
\[
b_{i,j} = |u_0 v_{i,j-1}| + |u_1 v_{i,j-2}| + \ldots + |u_i v_{i,j-i-1}|
\]
(2)

where \( l = \min(i-1, j-1) \), if \( r > n \), and \( l = 0 \) if \( r > n \), and \( |u_l v_j| = u_l v_j - u_j v_l \).

The next two theorems, presented in [9, 10], refer to the properties of the GCD of polynomials through Bézout matrices.

Theorem 1. Let \( f(s) \) and \( g(s) \) two polynomials in one variable as given in Definition 1. The greatest common divisor of the polynomials \( f(s) \) and \( g(s) \), denoted by \( \gcd(f(g)) \), is a polynomial with degree \( \deg(\gcd(f,g)) \leq p \) such that
\[
\dim \{ \text{NullSpace} \{ B(f, g) \} \} = \deg(\gcd(f,g)) = n - \text{rank} \{ B(f, g) \}
\]
(3)

Theorem 2. If \( c_1, c_2, \ldots, c_n \) are the columns of the Bézout matrix \( B(f, g) \) with rank \( n - k \), then

i) the last \( n - k \) columns, i.e. \( c_{k+1}, \ldots, c_n \), are linearly independent, and

ii) every column \( c_i \) for \( i = 1, 2, \ldots, k \) can be written as a linear combination of \( c_{k+1}, \ldots, c_n \):
\[
c_{k-i} = \sum_{j=k+1}^{n} h_{k-i}^{(j)} c_j, \quad i = 0, 1, \ldots, k - 1
\]
(4)

iii) There are \( d_1, d_2, \ldots, d_k \) such that \( d_j = d_k \cdot h_{k-j}^{(k)} \) and
\[
\begin{bmatrix}
    d_k \\
    d_{k-1} \\
    d_{k-2} \\
    \vdots \\
    d_0
\end{bmatrix} = d_k \begin{bmatrix}
    1 \\
    h_{k}^{(k-1)} \\
    h_{k-1}^{(k-1)} \\
    \vdots \\
    h_1^{(k-1)}
\end{bmatrix}
\]
(5)

with \( d_0 \) a non-zero real number.

Then, the GCD of the polynomials \( f \) and \( g \), denoted by \( \gcd(f, g) \), is
\[
\gcd(f, g) = d_0 s^k + d_1 s^{k-1} + \ldots + d_{k-1} s + d_k
\]
(6)

Remark 1. Let \( f, g \) be two polynomials of degree \( n \) and \( p \), respectively, and let \( k = \max\{n, p\} \). Then \( \deg(\gcd(f,g)) = k - \text{rank}(B(f, g)) \) or equivalently \( \text{rank}(B(f, g)) = k - \deg(\gcd(f,g)) < k \). The equality holds when the polynomials are coprime. Otherwise, \( \text{rank}(B(f, g)) < k \), which means that the Bézout matrix is rank deficient.
An important issue arising from Theorem 2 is the determination of the coefficients of the GCD of the entire set of polynomials. Next, exploiting the rank deficiency property of the Bézout matrix when a non-trivial GCD exists, we propose the application of the rank revealing QR factorization to a Bézout matrix.

Theorem 3. (QR factorization with column pivoting (QRCP) for rank deficient Bézout matrices). Let \( B \in \mathbb{R}^{n \times n} \) and \( \text{rank}(B) = r < n \), where \( B \) is a Bézout matrix as defined in (1). Then, there always exist a permutation matrix \( P \) of order \( n \) and a \( n \times n \) orthogonal matrix \( Q \) [12] such that

\[
Q^T B P = R = \begin{bmatrix}
R_{11} & R_{12} \\
0 & 0
\end{bmatrix}
\begin{bmatrix}
r \\
n-r
\end{bmatrix}
\]

where \( R_{11} \) is an \( r \times r \) upper triangular matrix with non-zero diagonal elements. Furthermore, if \( B \tilde{P} = [\tilde{b}_{c_1}, \tilde{b}_{c_2}, \ldots, \tilde{b}_{c_n}] \) and \( Q = [q_1, \ldots, q_n] \) presented in column form, then

\[
\tilde{b}_{c_k} = \sum_{i=1}^{\min(r,k)} r_{ik} q_i \in \text{span}\{q_1, \ldots, q_r\}, \quad k = 1, 2, \ldots, n
\]

which implies that \( \text{range}(B) = \text{span}\{q_1, \ldots, q_r\} \).

Remark 2. Considering the values of \( r_{ik} \) in (8) as the values of \( h_k^{(i)} \) in (4), we can directly obtain the coefficients \( d_i \) of the gcd(\( f \), \( g \)) through the Bézout-QRCP method. (This is fully demonstrated in Example 1 in Section 3). The application of the QRCP method to Bézout matrices simultaneously reveals the rank and an orthogonal base for the range of the Bézout matrix. Thus, by following Theorem 2 the coefficients of the GCD can easily be determined in a more efficient way.

Considering the case of sets of several polynomials, the following definition of an extended form of the Bézout matrix is given.

Definition 2. We consider the set of \( m+1 \) real univariate polynomials:

\[
P_{m+1,n} = \left\{ a(s), b_1(s), \ldots, b_m(s) \in \mathbb{R}[s], \quad i = 1, 2, \ldots, m \right\}
\]

with \( n = \deg\{a(s)\} \)

\[
p = \max_{i=1,\ldots,m} \{\deg\{b_i(s)\}\} \leq n
\]

Definition 3. Let \( u, v_1, \ldots, v_m \) be \( m+1 \) polynomials, with \( u \) a polynomial of maximal degree \( n \). Let \( B_i \) be the Bézout matrix of polynomials \( u, v_i \), for \( i = 1, \ldots, n \). Then the generalized Bézout matrix is defined as follows:

\[
B = \begin{bmatrix}
B_1 \\
B_2 \\
\vdots \\
B_n
\end{bmatrix} \in \mathbb{R}^{mn \times n}
\]

Remark 3. Theorems 1, 2, and 3 also hold for the generalized Bézout matrix.

2.2 Representation of the GCD through Sylvester matrices

Let \( \mathbb{R}[s] \) be the ring of real polynomials in one variable. We consider two polynomials \( a(s), b(s) \in \mathbb{R}[s] \), with degrees \( \deg\{a(s)\} = n \) and \( \deg\{b(s)\} = p \), respectively, where \( p \leq n \).

\[
a(s) = a_n s^n + a_{n-1} s^{n-1} + \ldots + a_1 s + a_0, \quad a_n \neq 0
\]

\[
b(s) = b_p s^p + b_{p-1} s^{p-1} + \ldots + b_1 s + b_0, \quad b_p \neq 0
\]
The resultant matrix or Sylvester matrix $S \in \mathbb{R}^{(n+p) \times (n+p)}$ of the two polynomials $a$ and $b$ is defined by

\[
S = \begin{bmatrix}
a_n & a_{n-1} & \cdots & a_{n-p} & a_{n-p-1} & \cdots & a_0 & 0 & \cdots & 0 & 0 \\
0 & a_n & a_{n-1} & \cdots & a_{n-p} & \cdots & a_0 & 0 & \cdots & 0 & 0 \\
\vdots & \vdots & \ddots & \vdots & \cdots & \cdots & \vdots & \vdots & \ddots & \cdots & \vdots \\
0 & 0 & 0 & \cdots & a_n & a_{n-1} & \cdots & a_1 & a_0 & \cdots & 0 \\
b_p & b_{p-1} & \cdots & b_0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 \\
0 & b_p & b_{p-1} & \cdots & b_0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & b_p & b_{p-1} & \cdots & b_1 & b_0 & \cdots & 0 \\
0 & 0 & 0 & \cdots & 0 & b_p & b_{p-1} & \cdots & b_1 & b_0 & \cdots & 0 \\
0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & b_p & b_{p-1} & \cdots & 0 \\
0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\
\end{bmatrix} = \begin{bmatrix}
S_0 \\
S_1 
\end{bmatrix}
\] (11)

**Theorem 4** ([20]). Let $a(s), b(s) \in \mathbb{R}[s]$, $\deg(a(s)) = n$, $\deg(b(s)) = p$, where $n \geq p$, and let
\[
g(s) = s^n + d_{k-1}s^{k-1} + \ldots + d_1s + d_0
\]
be their GCD. The following properties hold true:

i) $(a(s)$ and $b(s)$) are coprime, if and only if $\text{rank}(S) = n + p$.

ii) $k = \deg(d(s)) = n + p - \text{rank}(S)$

iii) If $S = Q \cdot R$ is the QR factorization of $S$, then the last non-vanishing row of $R$ gives the coefficients of GCD of the pair $(a(s), b(s))$.

In order to reduce the computational complexity of the QR factorization applied to $S$, we construct the modified Sylvester matrix, $S^\ast$, through row interchanges as it is described in [26]. The form of $S^\ast$ is the following:

\[
S^\ast = \begin{bmatrix}
a_n & a_{n-1} & \cdots & a_{n-p} & a_{n-p-1} & \cdots & a_0 & 0 & \cdots & 0 & 0 \\
b_p & b_{p-1} & \cdots & b_0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 \\
0 & a_n & a_{n-1} & \cdots & a_{n-p} & \cdots & a_1 & a_0 & 0 & \cdots & 0 \\
0 & b_p & b_{p-1} & \cdots & b_0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots & \cdots & \cdots & \vdots & \vdots & \ddots & \cdots & \vdots \\
0 & 0 & 0 & a_n & a_{n-1} & \cdots & a_{n-p} & a_{n-p+1} & a_{n-p} & a_{n-p-1} & \cdots & a_0 \\
0 & 0 & 0 & b_p & b_{p-1} & \cdots & b_0 & 0 & \cdots & 0 & 0 \\
0 & 0 & 0 & 0 & b_p & b_{p-1} & \cdots & b_1 & b_0 & 0 & \cdots & 0 \\
0 & 0 & 0 & 0 & 0 & b_p & b_{p-1} & \cdots & b_1 & b_0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & b_p & b_{p-1} & \cdots & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\
\end{bmatrix}
\] (12)

The following result provides a matrix representation of the standard factorization of the GCD of a set of several polynomials based on Sylvester and Toeplitz-like matrices.

**Definition 4.** We consider the set of polynomials $\mathcal{P} \equiv \mathcal{P}_{m+1,n}$ as defined in (9):

i) We can define a $p \times (n + p)$ matrix associated with $a(s)$:

\[
S_0 = \begin{bmatrix}
a_n & a_{n-1} & a_{n-2} & \cdots & a_1 & a_0 & 0 & \cdots & 0 \\
0 & a_n & a_{n-1} & \cdots & a_1 & a_0 & \cdots & \cdots & \cdots \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \cdots & \cdots \\
0 & 0 & 0 & a_n & a_{n-1} & \cdots & \cdots & \cdots & a_1 & a_0 
\end{bmatrix}
\] (13)
and $n \times (n + p)$ matrices associated with each $b_i(s)$, $i = 1, 2, \ldots, m$:

$$S_i = \begin{bmatrix}
    b_{i,p} & b_{i,p-1} & b_{i,p-2} & \cdots & b_{i,1} & b_{i,0} & 0 & \cdots & 0 \\
    0 & b_{i,p} & b_{i,p-1} & \cdots & b_{i,1} & b_{i,0} & \ddots & \vdots & \\
    \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\
    0 & \cdots & 0 & b_{i,p} & b_{i,p-1} & \cdots & b_{i,1} & b_{i,0}
\end{bmatrix} \quad (14)$$

A generalized Sylvester matrix or generalized resultant for the set $\mathcal{P}$ is defined by:

$$S_{\mathcal{P}} = \begin{bmatrix}
    S_0 \\
    S_1 \\
    \vdots \\
    S_m
\end{bmatrix} \in \mathbb{R}^{(mn+p) \times (n+p)} \quad (15)$$

ii) The matrix $S_{\mathcal{P}}$ is the basis matrix of the set of polynomials

$$S[\mathcal{P}] = \{ a(s), sa(s), \ldots, s^{p-1}a(s); b_1(s), \ldots, b_m(s), sb_m(s), \ldots, s^{n-1}b_m(s) \}$$

which is also referred to as the Sylvester Resultant set of the given set $\mathcal{P}$, [11, 29].

Theorem 4 also holds for the generalized Sylvester matrix $S_{\mathcal{P}}$ which has a special structure. By reordering its blocks through row-interchanging, we can construct the modified generalized Sylvester matrix $S_{\mathcal{P}}^*$ which has $n$
same blocks [26]. Thus, it can be handled more efficiently in respect of the required number of floating-point operations during the implementation of the QR factorization.

\[
S_p^* = \begin{bmatrix}
  b_{1p} & b_{1,p-1} & \ldots & b_{1,0} & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 \\
  b_{2p} & b_{2,p-1} & \ldots & b_{2,0} & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 \\
  \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
  b_{mp} & b_{m,p-1} & \ldots & b_{m,0} & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 \\
  0 & b_{1p} & \ldots & b_{1,1} & b_{1,0} & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 \\
  0 & b_{2p} & \ldots & b_{2,1} & b_{2,0} & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 \\
  \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
  0 & 0 & \ldots & 0 & b_{1p} & \ldots & b_{1,1} & b_{1,0} & 0 & 0 & \ldots & 0 \\
  0 & 0 & \ldots & 0 & b_{2p} & \ldots & b_{2,1} & b_{2,0} & 0 & 0 & \ldots & 0 \\
  \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
  0 & 0 & \ldots & 0 & b_{mp} & \ldots & b_{m,1} & b_{m,0} & 0 & 0 & \ldots & 0 \\
  0 & 0 & \ldots & 0 & 0 & b_{1p} & \ldots & b_{1,2} & b_{1,1} & b_{1,0} & 0 & \ldots & 0 \\
  0 & 0 & \ldots & 0 & 0 & b_{2p} & \ldots & b_{2,2} & b_{2,1} & b_{2,0} & 0 & \ldots & 0 \\
  \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
  0 & 0 & \ldots & 0 & b_{mp} & \ldots & b_{m,2} & b_{m,1} & b_{m,0} & 0 & 0 & \ldots & 0 \\
  0 & 0 & \ldots & 0 & b_{mp} & \ldots & b_{m,2} & b_{m,1} & b_{m,0} & 0 & 0 & \ldots & 0 \\
  \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
  a_n & a_{n-1} & \ldots & a_{n-p} & a_{n-p-1} & a_{n-p-2} & \ldots & a_2 & a_1 & a_0 & 0 & \ldots & 0 \\
  0 & a_n & \ldots & a_{n-p+1} & a_{n-p} & a_{n-p-1} & \ldots & a_3 & a_2 & a_1 & a_0 & \ldots & 0 \\
  \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
  0 & 0 & \ldots & 0 & 1 & a_{m-1} & \ldots & a_{m-n+1} & a_{m-n} & a_{m-n-1} & a_{m-n-2} & \ldots & a_0 \\
\end{bmatrix}
\]

(16)
2.3 Representation of the GCD through a power-basis matrix

We consider again a set of real polynomials in one variable as defined in (9). The polynomials \( b_i(s) \) are presented with respect to the maximum degree \( n \) of the leading polynomial \( a(s) \) as

\[
b_i(s) = \sum_{j=0}^{n} b_j^{(i)} s^j = \begin{bmatrix} b_0^{(i)} \\ b_1^{(i)} \\ \vdots \\ b_n^{(i)} \end{bmatrix}
\]

where \( d_i = \text{deg}(b_i(s)) \), \( b_{d_i}^{(i)} \neq 0 \) for every \( i = 1, 2, \ldots, m \) and \( b_p^{(i)} \neq 0 \) for at least one \( i \in \{1, \ldots, m\} \), since \( p = \max_{1 \leq i \leq m} d_i \). Then, for any set \( P_{m+1,n} \), a vector representative \( \bar{p}(s) \) and an associated matrix \( P_{m+1} \in \mathbb{R}^{(m+1) \times (n+1)} \) are defined by

\[
\bar{p}(s) = [a(s), b_1(s), \ldots, b_m(s)]^T = [a, b_1, \ldots, b_{m-1}, b_m]_s^T \cdot e_n(s) = P_{m+1} \cdot e_n(s)
\]

where \( e_n(s) = [s^n, s^{n-1}, \ldots, s, 1]^T \) and \( a, b_i \in \mathbb{R}^{n+1} \) for all \( i = 1, 2, \ldots, m \).

The next theorem [7] provides a representation of the GCD by using a matrix which is constructed directly from the coefficients of the polynomials according to a power-basis vector.

**Theorem 5.** Let \( P_{m+1,n} \) a set of \( m \) real univariate polynomials of maximum degree \( n \in \mathbb{N} \) and \( P_{m+1} \in \mathbb{R}^{(m+1) \times (n+1)} \) the matrix which is constructed according to the power-basis vector \( e_n(s) \). The application of elementary row operations and shifting to \( P_{m+1} \) results in a matrix \( G \in \mathbb{R}^{(m+1) \times (n+1)} \) with rank\( G = 1 \), which satisfies the equation:

\[
G = R \cdot P_{m+1} \cdot S
\]

where \( R \in \mathbb{R}^{(m+1) \times (m+1)} \) and \( S \in \mathbb{R}^{(n+1) \times (n+1)} \) represent the applied elementary row operations and the application of the shifting operation, respectively. The last non-zero row of \( G \) provides the coefficients of the GCD of the set \( P_{m+1,n} \).

**Remark 4.** It is important to stress that the shifting matrix \( S \) does not affect the numerical GCD solution, but it plays a significant role when a symbolic form of the GCD is under consideration. Therefore, it is always computed in symbolic-rational form (for more details the interested reader may refer to [7]).

The advantages of the representation of the GCD through a power-basis matrix are the following:

i) **Implementation using symbolic-rational computations.**

The relation (18) is particularly useful when symbolic-rational computations are involved, because it provides a compact way to represent the GCD solution as a product of matrices with the least possible dimensions allowed by the input data (see [7] for more details).

ii) **Handling multivariate polynomials.**

Recent experimental results showed that (18) provides a direct way to compute the GCD of sets of multivariate polynomials, when the procedure that constructs the initial matrix is appropriately adjusted. Considering the case of sets of \( m + 1 \) polynomials in two variables \( (s, t) \) (bivariate polynomials) with real coefficients, the \( n \times r \)-basis matrix \( P_{m+1} \) can be formed according to the bivariate power-basis:

\[
E_{n,r}(s, t) = \{ (1, t, \ldots, t^r), (s, st, \ldots, st^r), \ldots, (s^n, s^n t, \ldots, s^n t^r) \}
\]

where \( n, r \) are the maximum powers of the variables \( s, t \), respectively. The dimension of the corresponding basis vector \( E_{n,r}(s, t) \) is equal to \((n + 1) \cdot (r + 1)\). Similar base vectors can be formed for polynomials in several variables.
If we consider the column vectors $e_n(s) = [s^n, \ldots, s, 1]^T$ and $e_r(t) = [t^r, \ldots, t, 1]^T$, then the matrix $P_{m+1}$ is structured according to the bivariate power-basis vector:

$$e_{n,r}(s, t) = \begin{bmatrix}
t' & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
t & 0 & \cdots & 0 \\
1 & 0 & \cdots & 0 \\
0 & t^r & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & t & \cdots & 0 \\
0 & 1 & \cdots & 0 \\
\vdots & \ddots & \ddots & \vdots \\
0 & \cdots & 0 & t^r \\
0 & \cdots & 0 & 1
\end{bmatrix} \begin{bmatrix}
s^n \\
\vdots \\
s^n t \\
\vdots \\
s t \\
1 \\
\vdots \\
1
\end{bmatrix} = \begin{bmatrix}
ts^n t \\
\vdots \\
t \\
\vdots \\
t^r \\
1
\end{bmatrix}$$

If we consider the power-basis vectors $e_{n,r}(s, t)$ and $e_{n-r+n+1}(s)$, we can see that both vectors can yield the same power-basis matrix $P_{m+1}$ for a given set of polynomials. Therefore, we may assume a one-to-one correspondence between the two power-basis vectors, and if we apply Theorem 5 to a set of bivariate polynomials of degrees $(n, r)$, we can treat them as polynomials of maximum degree $n r + n + r$ and the column dimension of the matrix $P_{m+1}$ will be equal to $(n + 1)(r + 1)$. An analytical example for the case of bivariate polynomials is presented in the appendix.

3 Implementation of the GCD computation through matrix factorizations

The computation of the degree of the GCD of polynomials is an issue of great importance in GCD computations. The computation of the coefficients of the GCD depend on the correct determination of the degree of the GCD either in the Sylvester, or the Bézout case. In both cases QR factorization can be used for the efficient computation of the Sylvester matrix $S_p$ and the Bézout matrix $B$. However, several other approaches have been proposed for the computation of the degree of the GCD for the specific types of matrices.

Winkler et al. [28] proposed two methods for the calculation of the degree of the GCD of polynomials. The first method is based on the two subspaces that are enabled from the partitioned structure of the Sylvester matrix. The degree of the GCD is computed through monitoring the change of the angle of these two subspaces, by deliting rows and columns of the Sylvester matrix. The second method is based on considering the change in the error between two estimates of the GCD of the polynomials as a function of its degree. The properties and the application of the Sylvester matrix to GCD computations is also studied in [27].

Kaltofen et al. [15] presented a different method based on structured total least norm (STLN) algorithms applied to Sylvester matrices for computing the GCD of polynomials and Bini and Boito [4] presented a fast algorithm for computing the GCD of two polynomials, which uses Bézout and Sylvester matrices. More particularly, this algorithm is based on the reduction of their displacement structure to Cauchy-like one.

3.1 Computational complexity

Next, we analyze the numerical complexity of QR-based methods applied to the generalized Sylvester or the Bézout matrices. These factorizations compute an orthogonal matrix $Q$ and an upper triangular matrix $R$
which can produce the coefficients of the GCD of the polynomials. The computational complexity is measured in \textit{flops}, where 1-flop corresponds to the computational time required for one multiplication and one addition of floating point numbers.

### 3.1.1 Computation of the GCD through QR factorization

#### a) Sylvester-QR factorization

\textbf{Theorem 6} ([2, 3]). Let $S_p$ be the generalized Sylvester matrix of $m+1$ polynomials. If $S_p = QR$ is the QR factorization of $S_p$, the last non-zero row of $R$ gives the coefficients of the GCD of the polynomials.

The complexity of the QR factorization applied to $S_p$ is high. More precisely, for $m+1$ polynomials of maximum degree $n$ and second maximum degree $p$ the generalized Sylvester matrix is of size $(mn + p) \times (n + p)$ and thus, the required complexity is

$$O((n + p)^2 (mn + p - \frac{n + p}{3}))$$ \hspace{1cm} (21)

flops. If $m \simeq n \simeq p$ the complexity is $O(4n^4)$.

The modified Sylvester matrix $S_*^p$ has $n$ same blocks and, if we properly exploit the special structure of $S_*^p$ (see (16)) in QR factorization, the required complexity is decreased to

$$O((n + p)^3 (2 \log_2 n - \frac{1}{3}) + (n + p)^2 (2m \log_2 n + p))$$ \hspace{1cm} (22)

flops. If $m \simeq n \simeq p$, the required flops are about $O(16n^3 \log_2 n)$, [26].

#### b) Bézout-QR factorization

\textbf{Theorem 7} ([6]). Let $B$ be the generalized Bézout matrix of $m+1$ polynomials. If $JBJ = QR$ is the QR factorization of $JBJ$, where $J$ a permutation matrix with ones in its anti-diagonal and zeros elsewhere, then the last non-zero row of $R$ gives the coefficients of the GCD of the polynomials.

The complexity of the previous factorization for a $mn \times n$ Bézout matrix is $O(2n^2(mn - \frac{n}{2}))$ flops and, if $m \simeq n$, the required flops are about $O(2n^4)$.

### 3.1.2 Computation of the GCD through QR factorization with column pivoting (Bézout-QRCP method)

Since the $mn \times n$ Bézout $B$ matrix is always rank deficient when a non-trivial GCD exists, it is more efficient to extract the coefficients $h_i$ appeared in (4) using Remark 2, which indicates that the coefficients of the GCD of the polynomials can be derived from the QRCP factorization of the Bézout matrix. The complexity of the QRCP factorization is

$$O\left(2mn^2r - r^2(mn + n) + \frac{2r^3}{3}\right)$$ \hspace{1cm} (23)

flops [8], where $r$ is the rank of $B$, which is less than the flops required by the classical QR factorization. The appropriate correspondence of the columns of the original and the permuted matrix, which reveal the GCD coefficients (Remark 2), is symbolically implemented. In the case where the rank deficiency of $B$ is high, the Bézout-QRCP method becomes more efficient.

### 3.1.3 Computation of the GCD through Singular Value Decomposition (Subspace method)

A similar approach with Sylvester-like matrices is the method presented in [23]. Given a set of univariate polynomials $p_{m+1,n}$, the first two steps of the developed algorithm in [23] involves the construction of an
(m + 1)(n + 1) \times (2n + 1) \times (2n + 1) generalized Sylvester matrix\(^{1}\) \(\hat{S}_p\) from the input polynomials (as demonstrated in Example 2) and the computation of the left null space of the transposed \(\hat{S}_p^T\) via singular value decomposition. If we denote by \(U_0 \in \mathbb{R}^{(2n+1) \times k}\) the basis matrix for the computed left null space of \(\hat{S}_p^T\) and \(C\) is the \((2n + 1) \times (2n + 1 - k)\) Toeplitz matrix of a polynomial of degree \(k\) with arbitrary coefficients, then the GCD vector is actually the unique (up to a scalar) solution of the system \(U_0^T C = 0\). The degree of the GCD is \(k = \dim \{\text{range}(U_0)\}\). The computational cost of this method, which generally is rather high, is dominated by the singular value decomposition of the generalized Sylvester matrix \(\hat{S}_p\), which requires \(O(2m^2n^3 + 5m^2n^2)\) flops. If \(m \simeq n\) the required flops are about \(O(2n^3)\).

### 3.1.4 Remarks upon the computational complexity of the methods

Table 1 summarizes the required computational complexity for each of the aforementioned methods.

As it is shown in Table 1, for a given polynomial set \(P_{m+1,n}\), the complexity of the Sylvester and the modified Sylvester QR is a function of the maximum polynomial degrees \(n\) and \(p\). The required flops of the modified Sylvester QR are significantly less than that of the classical Sylvester QR. When \(p \ll n\) the complexity of the modified Sylvester QR can be further reduced. If \(n \simeq p\), the Sylvester QR method requires \(O(4n^3m)\) flops, while for its modified version \(O(4n^3(4 \log_2 n + \frac{1}{2}) + 8n^2m \log_2 n)\) flops are needed. Since \(\log_2 n\) becomes significantly less than \(n\) as the degree \(n\) increases, the modified Sylvester QR becomes more and more efficient than the classical one for higher degrees \(n\). When \(m \simeq n \simeq p\), the complexity of the modified method is decreased by one order comparing to the complexity of the classical method. The modified Sylvester QR has remarkable performance when applied to sets of many polynomials with high degrees.

The Bézout QRCP exploits the rank deficiency \(n - r\) of the matrices, which is equal to the degree of the GCD of the polynomials. Thus, the higher the GCD degree is (i.e. higher rank deficiency of the Bézout matrix) the more efficient the method becomes. If the rank of the Bézout matrix \(r\) is significantly less than the maximum degree \(n\) of the polynomials, then the complexity of the Bézout QRCP method is one order less comparing to the complexity of the classical Bézout QR. When \(m \simeq n \simeq p\), the complexity of the Bézout QRCP method is less than that of the modified Sylvester QR for \(r < 2\) \((6 \log_2 n + \frac{1}{2})\).

The subspace method requires significantly more floating-point operations than the other methods. This disadvantage is offset by the fact that this method gives more accurate values (i.e. lower relative errors) for the coefficients of the computed GCD comparing to the other methods.

### 3.2 Demonstrative Examples

The following example demonstrates the steps of the current Bézout-QRCP method for computing the GCD of set of many polynomials.

**Example 1.** We consider the pair of real univariate polynomials of degree 5:

\[
P_{2,5} = \begin{cases} 
  p_1(s) = s^5 - 24s^4 + 208s^3 - 786s^2 + 1231s - 630 \\
  p_2(s) = s^5 - 23s^4 + 195s^3 - 745s^2 + 1244s - 672 
\end{cases}
\]  

\(\text{(24)}\)

---

\(^{1}\) We must note that the constructed matrix \(\hat{S}_p\), although it is defined as a generalized Sylvester matrix in [23], it is slightly different than the matrix defined by (15), because the second maximum degree \(p\) of the polynomials is not considered at all.
Table 1: Computational complexity of methods computing the GCD of a polynomial set $P_{m+1,n}$ of maximum degree $n$ and second maximum degree $p$, where $r$ is the rank of the Bézout or the Sylvester matrix.

| Algorithm     | Complexity                                                                 | Complexity                          | Complexity                          |
|---------------|----------------------------------------------------------------------------|-------------------------------------|-------------------------------------|
| Sylvester QR  | $(n+p)^2 \left( (mn+p) - \frac{n+p}{r} \right)$                         | $4n^3 (m + \frac{1}{2})$           | $4n^4$                             |
| Modified Sylvester QR | $(n+p)^3 \left( 2\log_2 n - \frac{1}{2} \right) + (n+p)^2 (2m \log_2 n + p)$ | $4n^3 (4 \log_2 n + \frac{1}{2}) + 8n^2 m \log_2 n$ | $4n^3 (6 \log_2 n + \frac{1}{2})$ |
| Bézout QR     | $2n^2(mn - \frac{4}{2})$                                                  | $2n^2(mn - \frac{4}{2})$           | $2n^4$                             |
| Bézout QRCP   | $2mn^2r - r^2(mn + n) + \frac{2r^3}{3}$                                   | $2mn^2r - r^2(mn + n) + \frac{2r^3}{3}$ | $2n^3r - n^2r^2$                   |
| Subspace SVD  | $2m^2n^3 + 5m^2n^2$                                                       | $2m^2n^3 + 5m^2n^2$                 | $2n^5$                             |
The exact GCD is $s^2 - 8s + 7$. The Bézout matrix of the given polynomials in the set $\mathcal{P}_{2,5}$ is

$$B = \text{Bez}(p_1, p_2) = \begin{bmatrix} -1 & 13 & -41 & -13 & 42 \\ 13 & -145 & 185 & 1585 & -1638 \\ -41 & 185 & 3275 & -20345 & 16926 \\ -13 & 1585 & -20345 & 77615 & -58842 \\ 42 & -1638 & 16926 & -58842 & 43512 \end{bmatrix}$$ \hspace{1cm} (25)

where $b_{c_i}$, $i = 1, 2, \ldots, 5$ are the columns of the initial Bézout matrix $B \in \mathbb{R}^{5 \times 5}$.

The following factorization is achieved by applying the QR factorization with column pivoting (QRCP) to $B$, such that

$$B \Pi = QR$$ \hspace{1cm} (26)

where

$$Q = \begin{bmatrix} -0.0001306 & 0.017252 & 0.12062 & 0.52198 & -0.84421 \\ 0.015928 & -0.23579 & -0.85628 & -0.32276 & -0.32674 \\ -0.20444 & 0.83472 & 0.029962 & -0.44344 & -0.25281 \\ 0.77995 & -0.13851 & 0.31873 & -0.46068 & -0.24225 \\ -0.5913 & -0.47767 & 0.38697 & -0.46314 & -0.24074 \end{bmatrix}$$ \hspace{1cm} (27)

$$R = \begin{bmatrix} 99513 & -26543 & 2164.6 & -75109 & -26.384 \\ 0 & -2577.6 & 751.71 & 1881.4 & -55.567 \\ 0 & 0 & 2.6078 & -2.2362 & -0.37162 \\ 0 & 0 & 0 & 7.2816 \cdot 10^{-12} & 2.0961 \cdot 10^{-14} \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$ \hspace{1cm} (28)

and

$$\Pi = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$ \hspace{1cm} (29)

After applying the QRCP factorization, the permuted Bézout matrix $B_{\text{perm}} = B \cdot \Pi$ is

$$B_{\text{perm}} = \begin{bmatrix} -13 & 13 & 42 & -1 \\ 1585 & 185 & -145 & -1638 \\ -20345 & 3275 & 185 & 16926 \\ 77615 & -20345 & 1585 & -58842 \\ -58842 & 16926 & -1638 & 43512 \end{bmatrix}$$ \hspace{1cm} (30)

$$= \begin{bmatrix} \tilde{b}_{c_1} & \tilde{b}_{c_2} & \tilde{b}_{c_3} & \tilde{b}_{c_4} & \tilde{b}_{c_5} \end{bmatrix} = \begin{bmatrix} b_{c_1} & b_{c_2} & b_{c_3} & b_{c_4} & b_{c_5} \end{bmatrix}$$

The lowest right $2 \times 2$ part of $R$ is considered to be zero and, thus, QRCP indicates that $r = \text{rank}(B) = 3$ and $\deg(\gcd(\mathcal{P}_{2,5})) = 5 - 3 = 2$.

From Theorem 2 we know that the last 3 columns of the initial Bézout matrix $B$ in (25), i.e. $b_{c_1}$, $b_{c_4}$, and $b_{c_5}$, are linear independent. Therefore, the first two columns of $B$, $b_{c_1}$ and $b_{c_2}$, can be written as a linear combination of $b_{c_1}$, $b_{c_4}$ and $b_{c_5}$. Thus, from (4) in Theorem 2 we have:

$$b_{c_2} = h_{2}^{(3)} b_{c_1} + h_{2}^{(4)} b_{c_4} + h_{2}^{(5)} b_{c_5}$$ \hspace{1cm} (31)

$$b_{c_1} = h_{1}^{(3)} b_{c_1} + h_{1}^{(4)} b_{c_4} + h_{1}^{(5)} b_{c_5}$$ \hspace{1cm} (32)
Let \( d_0s^2 + d_1s + d_2 \) be the GCD of the polynomials. The coefficients \( h_2^{(3)} \) and \( h_1^{(3)} \) give the coefficients \( d_1 \) and \( d_0 \), respectively, and the constant term \( d_2 \) is 1.

Using QRCP, the coefficients \( h_2^{(3)} \) and \( h_1^{(3)} \) of the GCD are derived from the correspondence of the columns of \( B \) and \( B_{perm} \). According to Theorem 3, the columns \( q_1 \), \( q_2 \) and \( q_3 \) of \( Q \) generate the range of \( B_{perm} \). From (8) we have:

\[
\begin{align*}
\tilde{b}_{c_1} &= b_{c_4} = R_{11}q_1 \\
\tilde{b}_{c_2} &= b_{c_5} = R_{12}q_1 + R_{22}q_2 \\
\tilde{b}_{c_3} &= b_{c_5} = R_{13}q_1 + R_{23}q_2 + R_{33}q_3 \\
\tilde{b}_{c_4} &= b_{c_5} = R_{14}q_1 + R_{24}q_2 + R_{34}q_3 \\
\tilde{b}_{c_5} &= b_{c_1} = R_{15}q_1 + R_{25}q_2 + R_{35}q_3
\end{align*}
\]

(33)

Since the columns \( b_{c_1} \) and \( b_{c_5} \) of the initial Bézout matrix \( B \) correspond to \( \tilde{b}_{c_1} \) and \( \tilde{b}_{c_5} \) of the permuted Bézout matrix \( B_{perm} \), respectively, it is necessary to express the columns \( b_{c_1} \) and \( b_{c_5} \) as linear combinations of the columns \( \tilde{b}_{c_1} \), \( \tilde{b}_{c_2} \), and \( \tilde{b}_{c_5} \). Since each column \( q_i \), \( i = 1, 2, 3 \) is given by an analytic formula as the solution of the lower triangular system, formed from the first, the second, and the fourth equation of (33), we symbolically substitute in the third and the fifth equation of (33) and we obtain:

\[
\begin{align*}
\tilde{b}_{c_1} &= R_{11}q_1 + R_{23}q_2 + R_{33}q_3 \\
\tilde{b}_{c_5} &= R_{15}q_1 + R_{25}q_2 + R_{35}q_3
\end{align*}
\]

(34)

(35)

Therefore, we conclude that

\[
\begin{align*}
\tilde{b}_{c_1} &= -1.14282712402397 \tilde{b}_{c_1} - 1.16326188998929 \tilde{b}_{c_1} - 1.16617476075485 \tilde{b}_{c_4} \\
\tilde{b}_{c_5} &= 0.142855765690511 \tilde{b}_{c_2} + 0.163268401615028 \tilde{b}_{c_1} + 0.166183704498703 \tilde{b}_{c_4}
\end{align*}
\]

and from the correspondence of the columns of \( B \) and \( B_{perm} \) we have:

\[
\begin{align*}
b_{c_1} &= \tilde{b}_{c_1} = -1.14282712402397 b_{c_1} - 1.16326188998929 b_{c_1} - 1.16617476075485 b_{c_4} \\
b_{c_5} &= \tilde{b}_{c_5} = 0.142855765690511 b_{c_2} + 0.163268401615028 b_{c_1} + 0.166183704498703 b_{c_4}
\end{align*}
\]

Thus,

\[
h_2^{(3)} = -1.14282712402397 \quad \text{and} \quad h_1^{(3)} = 0.142855765690511
\]

and we obtain the quadratic polynomial:

\[
0.142855765690511 s^2 - 1.14282712402397 s + 1
\]

If we convert it to a monic polynomial, dividing by 0.142855765690511, we finally compute the GCD of the polynomials in \( \mathbb{P}_{2,5} \). That is

\[
\gcd(\mathbb{P}_{2,5}) = 1.0 s^2 - 7.999866988216918 s + 7.000067481815496
\]

(36)

In the following, we consider the computation of the GCD using the Bézout-QR, Sylvester-QR, power-basis, and the subspace-SVD methods.

**Example 2.** Let us consider the next set of three univariate polynomials:

\[
\mathbb{P}_{3,3} = \begin{cases}
p_1(s) = s^3 - 6s^2 + 11s - 6 \\
p_2(s) = s^3 - 7s^2 + 14s - 8 \\
p_3(s) = s^3 - 8s^2 + 17s - 10
\end{cases}
\]

(37)

of degree 3. Their exact GCD is \( s^3 - 3s + 2 \).
i) GCD from Bézout matrices using QRCP decomposition

The generalized Bézout matrix of the given polynomials in the set \( p_{3,3} \) is

\[
B = \begin{bmatrix} B_1 \\ B_2 \end{bmatrix} = \begin{bmatrix} 1 & -3 & 2 \\ -3 & 9 & -6 \\ 2 & -6 & 4 \\ 2 & -6 & 4 \\ -6 & 18 & -12 \\ 4 & -12 & 8 \end{bmatrix} = \begin{bmatrix} b_{c_1} & b_{c_2} & b_{c_3} \end{bmatrix}
\]  

(38)

where

\[
B_1 = \text{Bez}\{p_1, p_2\} = \begin{bmatrix} 1 & -3 & 2 \\ -3 & 9 & -6 \\ 2 & -6 & 4 \end{bmatrix}
\]  

(39)

and

\[
B_2 = \text{Bez}\{p_1, p_3\} = \begin{bmatrix} 2 & -6 & 4 \\ -6 & 18 & -12 \\ 4 & -12 & 8 \end{bmatrix}
\]  

(40)

and \( c_1, c_2, c_3 \) are the columns of \( B \).

We apply the QRCP factorization to \( B \), such that

\[
B II = QR
\]

where

\[
Q = \begin{bmatrix} -0.1195 & -0.9008 & 0.0782 & 0.1362 & 0.0739 & 0.3796 \\ 0.3586 & 0.1955 & -0.1646 & 0.2821 & -0.5820 & 0.6228 \\ -0.2390 & -0.0528 & -0.9655 & -0.0125 & 0.0871 & -0.0140 \\ -0.2390 & 0.1333 & 0.0583 & 0.9320 & 0.1821 & -0.1407 \\ 0.7171 & 0.0188 & -0.1214 & 0.0791 & 0.6675 & 0.1371 \\ -0.4781 & 0.3597 & 0.1285 & -0.1636 & 0.4118 & 0.6552 \end{bmatrix}
\]  

(41)

\[
R = \begin{bmatrix} 25.0998 & -16.7332 & -8.3666 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}
\]

(42)

and

\[
II = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}
\]

where \( q_1, q_2, q_3, q_4, \) and \( q_5 \) are the columns of \( Q \). The lowest right \( 5 \times 2 \) part of \( R \) is zero and thus, QRCP indicates that \( r = \text{rank}(B) = 1 \). The degree of the GCD is \( \deg(\text{gcd}(p_{3,3})) = 3 - r = 2 \).

Theorem 2 denotes that the last column \( b_3 \) of the initial Bézout matrix \( B \) in (38) is linear independent and the other columns \( b_1 \) and \( b_2 \) are multiples of \( b_3 \). Working similarly with Example 1 we conclude that:

\[
\text{gcd}(p_{3,3}) = s^2 - 3.0000s + 2.0000
\]  

(43)
ii) GCD from Sylvester matrices using QR decomposition.

The generalized Sylvester matrix of the polynomials in \( P_{3,3} \), as defined by (15), is:

\[
S_p = \begin{bmatrix}
1 & -6 & 11 & -6 & 0 & 0 \\
0 & 1 & -6 & 11 & -6 & 0 \\
0 & 0 & 1 & -6 & 11 & -6 \\
1 & -7 & 14 & -8 & 0 & 0 \\
0 & 1 & -7 & 14 & -8 & 0 \\
0 & 0 & 1 & -7 & 14 & -8 \\
1 & -8 & 17 & -10 & 0 & 0 \\
0 & 1 & -8 & 17 & -10 & 0 \\
0 & 0 & 1 & -8 & 17 & -10
\end{bmatrix} \in \mathbb{R}^{9 \times 6} \tag{44}
\]

Applying the QR factorization (without column pivoting), we have \( S_p = QR \), where

\[
R = \begin{bmatrix}
-1.7321 & 12.1244 & -24.2487 & 13.8564 & 0 & 0 \\
0 & -2.2361 & 12.0748 & -20.5718 & 10.7331 & 0 \\
0 & 0 & -4.9193 & 17.1974 & -17.1567 & 4.8787 \\
0 & 0 & 0 & 6.6370 & -19.9110 & 13.2740 \\
0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix} \tag{45}
\]

\[
Q = \begin{bmatrix}
-0.1942 & 0.2127 & 0.3592 & 0.7691 & \ldots \\
0.3560 & -0.0765 & 0.2318 & 0.1750 & \ldots \\
-0.1942 & -0.3620 & 0.1161 & 0.0378 & \ldots \\
-0.2589 & 0.2836 & 0.4210 & 0.0930 & \ldots \\
0.4530 & -0.0783 & 0.3296 & 0.0079 & \ldots \\
-0.2265 & -0.4833 & 0.1875 & -0.0052 & \ldots \\
-0.3236 & 0.3545 & 0.4827 & -0.5831 & \ldots \\
0.5501 & -0.0802 & 0.4274 & -0.1591 & \ldots \\
-0.2589 & -0.6046 & 0.2588 & -0.0483 & \ldots \\
-0.1964 & -0.2508 & -0.0130 & 0.2563 & 0.1708 \\
0.6160 & -0.4654 & 0.1206 & -0.3090 & -0.2777 \\
-0.1741 & 0.0912 & 0.6073 & 0.2545 & -0.5866 \\
0.2894 & 0.6768 & -0.0215 & -0.3224 & -0.1428 \\
-0.6570 & 0.0256 & -0.0984 & -0.4668 & -0.1413 \\
0.0583 & -0.0379 & -0.7427 & 0.1606 & -0.3125 \\
-0.0930 & -0.4260 & 0.0345 & 0.0661 & -0.0280 \\
0.1444 & 0.2645 & 0.0253 & 0.5856 & 0.2202 \\
0.0578 & -0.0244 & 0.2298 & -0.2812 & 0.6019
\end{bmatrix} \tag{46}
\]

The last non zero row of \( R \) gives the coefficients of the GCD. If the fourth row of \( R \) is divided by the element \( R_{4,6} \), then

\[
gcd(P_{3,3}) = s^2 - 3.0000s + 2.0000.
\]
iii) GCD from Sylvester matrices using singular value decomposition.

A different approach [23] can be followed if we compute the left null space of the generalized Sylvester matrix \( \hat{S}_{p} \) by using the singular value decomposition \( \hat{S}_{p}^T = U \Sigma V^T \), where

\[
\hat{S}_{p} = \begin{bmatrix}
1 & -6 & 11 & -6 & 0 & 0 & 0 \\
0 & 1 & -6 & 11 & -6 & 0 & 0 \\
0 & 0 & 1 & -6 & 11 & -6 & 0 \\
0 & 0 & 0 & 1 & -6 & 11 & -6 \\
1 & -7 & 14 & -8 & 0 & 0 & 0 \\
0 & 1 & -7 & 14 & -8 & 0 & 0 \\
0 & 0 & 1 & -7 & 14 & -8 & 0 \\
1 & -8 & 17 & -10 & 0 & 0 & 0 \\
0 & 1 & -8 & 17 & -10 & 0 & 0 \\
0 & 0 & 1 & -8 & 17 & -10 & 0 \\
0 & 0 & 0 & 1 & -8 & 17 & -10 \\
\end{bmatrix} \in \mathbb{R}^{12 \times 7}
\]

\[
U = \begin{bmatrix}
-0.0146 & 0.0313 & -0.0520 & -0.0777 & -0.4255 & -0.0782 & -0.8960 \\
0.1251 & -0.2402 & 0.3344 & 0.3971 & 0.6734 & 0.2052 & -0.4020 \\
-0.3806 & 0.5520 & -0.4526 & -0.1902 & 0.4063 & 0.3468 & -0.1549 \\
0.5859 & -0.3464 & -0.3010 & -0.1549 & 0.0746 & 0.4177 & -0.0314 \\
-0.5783 & -0.3239 & 0.4530 & -0.3598 & -0.1408 & 0.4531 & 0.0303 \\
0.3833 & 0.5867 & 0.4477 & 0.1199 & -0.2619 & 0.4708 & 0.0612 \\
-0.1208 & -0.2597 & -0.4294 & 0.6255 & -0.3261 & 0.4797 & 0.0766 \\
\end{bmatrix}
\]

\[
\Sigma = \text{diag}(47.3732, 34.1874, 19.0932, 7.3558, 0.5852, 0.0000, 0.0000)
\]

Assuming \( U_0 \) contains the left null eigenvectors of the matrix \( U \), then the linear system \( U_0^T C = 0 \) provides the coefficients of the GCD in the vector form

\[
\begin{bmatrix}
0.267261241912424 \\
-0.801783725737273 \\
0.534522483824849
\end{bmatrix}
\]

which implies

\[
\text{gcd}(p_{3,3}) = s^2 - 3.0000000000000004 s + 2.0000000000000005
\]  

(50)

when we divide every element by 0.267261241912424.

iv) GCD from a power-basis matrix.

The power-basis matrix of the polynomials in the set \( p_{3,3} \) is

\[
P_3 = \begin{bmatrix}
1 & -6 & 11 & -6 \\
1 & -7 & 14 & -8 \\
1 & -8 & 17 & -10 \\
\end{bmatrix}
\]

(51)

for \( g_2(s) = [s^2, s, 1]^T \). If we apply Theorem 5 using symbolic-rational computations, we obtain the matrices

\[
R = \begin{bmatrix}
-1 & 1 & 0 \\
0 & 1 & 0 \\
0 & 0 & 0 \\
\end{bmatrix}, \quad S = \begin{bmatrix}
3104 & 5724 & -584 & 4672 \\
2645 & 2645 & 529 & 2645 \\
2645 & 1737 & 1117 & 586 \\
2645 & 1066 & 1174 & 1188 \\
2645 & 529 & 529 & 2645 \\
2645 & 2053 & 409 & 4124 \\
\end{bmatrix}
\]

(52)
and the rows of the matrix

\[ G = R \cdot P_3 \cdot S = \begin{bmatrix} 0 & -1 & 3 & -2 \\ 0 & -3 & 9 & -6 \\ 0 & 0 & 0 & 0 \end{bmatrix} \] (53)

provide the coefficients of the GCD up to a scalar multiple.

4 Numerical examples

In this section we compare the Bézout-QRCP method, which is proposed in this work, the Bézout-QR developed in [6], the Sylvester-QR for the modified case, and the subspace-SVD method [23]. All the aforementioned methods are based on numerically stable procedures such as QR decomposition (with or without column pivoting) and singular value decomposition [12] which are widely used in numerical applications and are included in high-performance computational software packages, such as Matlab and Maple.

We run several computational simulations in Matlab on an AMD-A6 Dual-Core 3.6 GHz - 8Gb machine using many different sets of polynomials with randomly selected coefficients in order to test the numerical behavior and performance of the described methods by measuring the processing time (Fig. 1) and the relative error (Fig. 2) when an exact GCD is known. The results obtained showed that, in general, all methods can provide reliable results within an acceptable range of accuracy.

Furthermore, those results were obtained after normalizing the rows of the input matrix (i.e. the elements each row are divided by the norm of the row) and were slightly better than those obtained without normalization. This is a scaling technique which is widely used and generally improves the accuracy of the results. In the current computational simulations we used the Euclidean norm. Two operations, scaling by the geometric mean and relative scaling are also suggested in [28]. These operations are applied to the coefficients of the initial polynomials before the factorization of the Sylvester or the Bézout matrix.

Example 3. In Table 2 and Table 3 we summarize the results obtained regarding the numerical relative error for the computed GCD of the polynomial sets in Example 1 and Example 2, respectively.

| Algorithm      | Tolerance       | Rel. Error   |
|----------------|-----------------|--------------|
| Bézout-QRCP    | $10^{-10} - 10^{-16}$ | $O \left( 10^{-13} \right)$ |
| Bézout-QR      | $10^{-10} - 10^{-16}$ | $O \left( 10^{-12} \right)$ |
| Sylvester-QR   | $10^{-10} - 10^{-16}$ | $O \left( 10^{-13} \right)$ |
| Subspace-SVD   | $10^{-10} - 10^{-14}$ | $O \left( 10^{-11} \right)$ |

The tolerance indicates the different levels of precision (numerical accuracy) where a number is considered to be zero. For the particular sets of polynomials a tolerance between $10^{-10}$ and $10^{-16}$ was selected with an exception for the subspace-SVD method which couldn’t determine the correct degree of the GCD when the tolerance was smaller than $10^{-16}$. 

\[ \square \]
Table 3: Numerical relative error for the GCD of the set (37) in Example 2.

| Algorithm       | Tolerance       | Rel. Error       |
|-----------------|-----------------|------------------|
| Bézout-QRCP     | $10^{-10} - 10^{-16}$ | $O\left(10^{-16}\right)$ |
| Bézout-QR       | $10^{-10} - 10^{-16}$ | $O\left(10^{-16}\right)$ |
| Sylvester-QR    | $10^{-10} - 10^{-16}$ | $O\left(10^{-16}\right)$ |
| Subspace-SVD    | $10^{-10} - 10^{-14}$ | $O\left(10^{-15}\right)$ |

Figure 1: Computational performance

Figure 2: Numerical efficiency
5 Conclusions

In this paper, we proposed the application of the QR factorization with column pivoting to a Bézout matrix in order to compute the coefficients of the GCD of sets of several polynomials in a more efficient way. We also presented an overview of the most frequently applied structured matrix-based representations: i) the Sylvester QR, ii) the Bézout QR, and iii) the subspace SVD method. All these methods start with a structured matrix constructed directly from the coefficients of the given polynomial set. The size of the block banded generalized Sylvester matrix is larger than that of the generalized Bézout, which consists of blocks of symmetric matrices. The subspace method involves a Sylvester-like matrix of biggest dimensions. Taking into account the structure of each of the above matrices, we compared the methods theoretically with respect to their computational complexity.

From this study, we can recommend the application of the most appropriate method according to the given polynomial set. Specifically, for a large set of polynomials with high degree, the modified Sylvester QR method is more preferable. As the number of the polynomials in the set decreases the Bézout QRCP becomes more efficient. Additionally, the results obtained from the simulations considering an exact GCD showed that both methods produced accurate results in reasonable time limits. However, the subspace-SVD method appears to be more stable for large sets of polynomials, but the processing time increases at a high rate as the number of polynomials increases.

The study of the approximate GCD case is also a topic of great interest. A thorough comparison among the existing methods and possible extension of the QRCP method to the approximate case is under consideration. Furthermore, a proper framework for the algebraic and geometric properties of the GCD of sets of many polynomials in a multidimensional space is currently under study in order to define and evaluate exact or approximate multivariate GCDs given by the QRCP method. This is a challenging problem for further research, because several real-time applications, such as image and signal processing, rely on GCD methods where multivariate polynomials (especially in two variables) are used.

Appendix

Computation of the GCD of a set of bivariate polynomials

The following example demonstrates the computation of a set of several bivariate polynomials through a power-basis vector based on the relation (18) in Theorem 5. We consider the set of polynomials:

\[ P = \{ \begin{aligned}
   p_1(s, t) &= (st - 3)(t + 1) = st^2 - 3t^2 + 5t - 2 \\
   p_2(s, t) &= (s - 3)(t + 2) = st - 5st + 2s + 6t - 4 \\
   p_3(s, t) &= (s - 3)(t - 3) = s^2t - 3st^2 - st + 9t - 6
\end{aligned} \]

with \( \gcd(P) = st - 3t + 2 \). The maximal power of the variable \( s \) is \( n = 2 \) and the maximal power of the variable \( t \) is also \( r = 2 \). Then, the initial power-basis matrix \( P_{m+1} \) for \( m + 1 = 3 \) and the power-basis vector of the variables \( s, t \) are

\[
P_{m+1} = \begin{bmatrix}
0 & 0 & 0 & 1 & -1 & 0 & -3 & 5 & -2 \\
0 & 1 & 0 & 0 & -5 & 2 & 0 & 6 & -4 \\
1 & 0 & 0 & -3 & -1 & 0 & 0 & 9 & -6
\end{bmatrix},
\]

\[ e_{2,2}(s, t) = \begin{bmatrix}
s^2t^2, s^2t, s^2t^2, st, st^2, s, t^2, t, 1
\end{bmatrix}^T \]
If we apply Theorem 5 using symbolic-rational computations, we finally obtain the matrices $R \in \mathbb{R}^{3 \times 3}$ and $S \in \mathbb{R}^{9 \times 9}$ as given in (54) and (55), respectively, where

$$R = \begin{bmatrix}
-\frac{3}{2} & -\frac{3}{2} & 1 \\
4 & 3 & -2 \\
-1 & 4 & -2
\end{bmatrix} \quad (54)$$

such that

$$S = \begin{bmatrix}
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\end{bmatrix} \quad (55)$$

$$G = R \cdot P_{m+1} \cdot S = \begin{bmatrix}
0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & \frac{3}{2} & -1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & -3 & 2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix} \quad (56)$$
The last non-zero row provides the coefficients of the GCD. Actually, any non-zero row of $G$ provides the GCD up to a scalar multiple. The GCD vector is

$$g = [0, 0, 0, 1, 0, 0, -3, 2]$$

and

$$\gcd(p) = g \cdot e_{2,2}(s, t) = s t - 3 t + 2$$

**Acknowledgement:** We would like to sincerely thank the reviewers for their comments and suggestions on the paper, as these comments led us to an improvement of the work.

**References**

[1] S. Barnett. Degrees of greatest common divisor of invariant factors of two regular polynomial matrices. In *Proc. Cambridge Philos. Soc.*, volume 66, pages 241–245, 1970.

[2] S. Barnett. Greatest common divisor of several polynomials. In *Proc. Cambridge Philos. Soc.*, volume 70, pages 263–268, 1971.

[3] S. Barnett. Greatest common divisor from generalized Sylvester matrices. In *Proc. Cambridge Philos. Soc.*, volume 8, pages 271–279, 1980.

[4] D. A. Bini and P. Boito. A fast algorithm for approximate polynomial gcd based on structured matrix computations. *Operator Theory: Advances and Applications*, 199:155–173, 2010.

[5] W. Blankship. A new version of Euclid’s algorithm. *American Mathematics Monthly*, 70:742–744, 1963.

[6] P. Boito. *Structured Matrix Based Methods for Approximate Polynomial GCD*. PhD thesis, Tesi di Perfezionamento in Matematica, Scuola Normale Superiore, Italy, 2007.

[7] D. Christou, N. Karcanias, and M. Mitrouli. Matrix representation of the shifting operation and numerical properties of the ERES method for computing the greatest common divisor of sets of many polynomials. *J. Comp. Appl. Math.*, 260:54–67, 2014.

[8] B. N. Datta. *Numerical Linear Algebra and Applications*. SIAM, Philadelphia, USA, 2nd edition, 2010.

[9] G. M. Diaz-Toca and L. Gonzalez-Vega. Barnett’s theorems about the greatest common divisor of several univariate polynomials through bezout-like matrices. *J. Symbolic Computation*, 34:59–81, 2002.

[10] G. M. Diaz-Toca and L. Gonzalez-Vega. Computing greatest common divisors and squarefree decompositions through matrix methods: The parametric and approximate cases. *Linear Algebra and its Applications*, 412:222–246, 2006.

[11] L. Foster. Rank and null space calculations using matrix decomposition without column interchanges. *Linear Algebra and its Applications*, 74:47–71, 1986.

[12] G. H. Golub and C. F. Van Loan. *Matrix Computations*. The John Hopkins University Press, Baltimore and London, 3rd edition, 1996.

[13] L. Gonzalez-Vega. An elementary proof of Barnett’s theorem about the greatest common divisor of several univariate polynomials. *Linear Algebra and its Applications*, 247:185–202, 1996.

[14] T. Kailath. *Linear Systems*. Prentice Hall, Inc., Englewood Cliffs, NJ, 1980.

[15] E. Kaltofen, Z. Yang, and L. Zhi. Structured low rank approximation of a sylvester matrix. *Symbolic-Numeric Computation, Trends in Mathematics*, pages 69–83, 2007.

[16] N. Karcanias and M. Mitrouli. A matrix pencil based numerical method for the computation of the gcd of polynomials. *IEEE Trans. Autom. Cont.*, 39:977–981, 1994.

[17] N. Karcanias and M. Mitrouli. Approximate algebraic computations of algebraic invariants. In *Symbolic methods in control systems analysis and design*, volume 56 of *IEEE Control Engin. Series*, pages 135–168. IET, Institute of Engineering and Technology, 1999.

[18] N. Karmarkar and Y. N. Lakshman. Approximate polynomial greatest common divisors and nearest singular polynomials. In *Proc. ISSAC’96*, pages 35–39, Zurich, Switzerland, 1996.

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

[20] M. Mitrouli N. Karcanias and S. Fatouros. A resultant based computation of the gcd of two polynomials. In *Proc. of 11th IEEE Mediterranean Conf. on Control and Automation*, Rhodes, Greece, 2003.

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

[22] I. S. Pace and S. Barnett. Comparison of algorithms for calculation of g.c.d of polynomials. *Int. J. Control*, 4(2):211–216, 1973.
[23] W. Qui, Y. Hua, and K. Abed-Meraim. A subspace method for the computation of the gcd of polynomials. *Automatica*, 33(4):255–284, 1997.

[24] H. Rosenbrock. *State Space and Multivariable Theory*. Nelson, London, 1970.

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

[26] D. Triantafyllou and M. Mitrouli. On rank and null space computation of the generalized sylvester matrix. *Numer. Algor.*, 54:297–324, 2010.

[27] J. R. Winkler. Polynomial computations for blind image deconvolution. *Linear Algebra App.*, 502:77–103, 2016.

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

[29] W. M. Wonham. *Linear Multivariable Control: A Geometric Approach*. Springer Verlag, New York, 2nd edition, 1984.