Approximate Greatest Common Divisor through factorization of matrices of special structure

Mitrouli Marilena[1] Triantafyllou Dimitrios[2]

[1]National and Kapodistrian University of Athens
Department of Mathematics
Panepistimiopolis, 15771 Ilissia, Greece
e-mail: mmitroul@math.uoa.gr
[2]Department of Mathematics and Engineering Sciences
Hellenic Military Academy
GR-16673, Vari, Greece
e-mail: dtriant@sse.gr

NASCA 2018, Kalamata, Greece

GCD and AGCD

Computation of the Greatest Common Divisor (GCD) and the Approximate GCD of a set of polynomials:

i. Image Deblurring
ii. Networks
iii. Secret Sharing Schemes
iv. Control Theory

Methods for Computing the GCD and AGCD of Polynomials:

i. Numerical methods based on Euclid's algorithm and its generalizations.
ii. Numerical-Hybrid methods based on procedures involving matrices of special structure.
iii. Numerical methods based on DFT.

GCD and AGCD

Difficulties:

i. Noise and measurement errors in initial data.

ii. Errors in numerical computations in Floating Point Arithmetic.

Possible Problems:

i. Inaccurate computation of the exact degree of the GCD.

ii. Inaccurate computation of the common factors of the GCD.

iii. Increase of the required time.

Need of:

Relaxation of the notion of the exact GCD and the computation of an approximate GCD (AGCD) of polynomials.

Introduction of the Problem

Let

$$a(x)=a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_0$$

be a polynomial of maximal degree n and $b_i(x)$, $i = 1, \ldots m$

$$b_i(x) = b_{i,k}\, x^p + b_{i,p-1}\, x^{p-1} + b_{i,p-2}\, x^{p-2} + \ldots + b_{i,0}$$

be m polynomials of maximal degree p, $p \leq n$.

Compute the

i. degree of the GCD or AGCD of polynomials.

ii. coefficients of the GCD or AGCD of polynomials.

Classical Generalized Sylvester matrix

$$S_0 = \begin{bmatrix} a_n & a_{n-1} & a_{n-2} & \dots & a_0 & 0 & \dots & 0 & 0 \\ 0 & a_n & a_{n-1} & \dots & a_1 & a_0 & \dots & 0 & 0 \\ . & . & . & \dots & . & . & \dots & . & . \\ 0 & 0 & 0 & a_n & \dots & . & . & a_1 & a_0 \end{bmatrix}$$

and

$$S_i = \begin{bmatrix} b_{i,p} & b_{i,p-1} & \dots & b_{i,0} & 0 & \dots & 0 \\ 0 & b_{i,p} & \dots & b_{i,1} & b_{i,0} & \dots & 0 \\ . & . & . & \dots & . & \dots & . \\ 0 & 0 & 0 & b_{i,p} & \dots & . & b_{i,0} \end{bmatrix}, \quad i = 1, \dots, m$$

Classical Generalized Sylvester matrix:

$$S = \begin{bmatrix} S_0 \\ S_1 \\ \vdots \\ S_m \end{bmatrix}$$

Modified Generalized Sylvester matrix

$$
\begin{bmatrix}
b_{1p} & b_{1,p-1} & b_{1,p-2} & \dots & b_{1,0} & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
b_{2p} & b_{2,p-1} & b_{2,p-2} & \dots & b_{2,0} & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
. & . & . & \dots & . & . & . & \dots & . & . & . & . & \dots & . \\
b_{mp} & b_{m,p-1} & b_{m,p-2} & \dots & b_{m,0} & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
0 & b_{1p} & b_{1,p-1} & \dots & b_{1,1} & b_{1,0} & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
0 & b_{2p} & b_{2,p-1} & \dots & b_{2,1} & b_{2,0} & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
. & . & . & \dots & . & . & . & \dots & . & . & . & . & \dots & . \\
0 & b_{mp} & b_{m,p-1} & \dots & b_{m,1} & b_{m,0} & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
. & . & . & \dots & . & . & . & \dots & . & . & . & . & \dots & . \\
0 & 0 & 0 & \dots & 0 & 0 & b_{1p} & \dots & b_{1,2} & b_{1,1} & b_{1,0} & 0 & \dots & 0 \\
0 & 0 & 0 & \dots & 0 & 0 & b_{2p} & \dots & b_{2,2} & b_{2,1} & b_{2,0} & 0 & \dots & 0 \\
. & . & . & \dots & . & . & . & \dots & . & . & . & . & \dots & . \\
0 & 0 & 0 & \dots & 0 & 0 & b_{mp} & \dots & b_{m,2} & b_{m,1} & b_{m,0} & 0 & \dots & 0 \\
. & . & . & \dots & . & . & . & \dots & . & . & . & . & \dots & . \\
. & . & . & \dots & . & . & . & \dots & . & . & . & . & \dots & . \\
0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & b_{1p} & b_{1,p-1} & 0 & \dots & b_{1,0} \\
0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & b_{2p} & b_{2,p-1} & 0 & \dots & b_{2,0} \\
. & . & . & \dots & . & . & . & \dots & . & . & . & . & \dots & . \\
0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & b_{mp} & b_{m,p-1} & 0 & \dots & b_{m,0} \\
a_n & a_{n-1} & a_{n-2} & \dots & a_{n-p} & a_{n-p-1} & a_{n-p-2} & \dots & a_2 & a_1 & a_0 & 0 & \dots & 0 \\
0 & a_n & a_{n-1} & \dots & a_{n-p+1} & a_{n-p} & a_{n-p-1} & \dots & a_3 & a_2 & a_1 & a_0 & \dots & 0 \\
. & . & . & \dots & . & . & . & \dots & . & . & . & . & \ddots & . \\
0 & 0 & 0 & \dots & 0 & a_n & a_{n-1} & \dots & a_{n-p+1} & a_{n-p} & a_{n-p-1} & a_{n-p-2} & \dots & a_0
\end{bmatrix}
$$

Modified Generalized Sylvester matrix

$$S^* = \begin{bmatrix} B\underline{00} & \mathbb{0} & & \\ \underline{0}B\underline{0} & \mathbb{0} & & \\ \underline{00}B & \mathbb{0} & & \\ & \ddots & \ddots & \\ & \mathbb{0} & & \underline{0}B \\ & S_0 & & \end{bmatrix}$$

Theorem

Perform LU or QR factorization to S or S^* and let U or R be the upper triangularization of them respectively. Then,

i. *$r = deg\,GCD =$ number of zero rows of U or R.*

ii. *The last non-zero row of U or R gives the coefficients of GCD of polynomials in reverse order.*

Skinny QR factorization

1st Step

$$Q_1^* S^* = \begin{bmatrix} Q_1^T & \mathbb{0} & \mathbb{0} & \dots & \mathbb{0} & \mathbb{0} \\ \mathbb{0} & Q_1^T & \mathbb{0} & \dots & \mathbb{0} & \mathbb{0} \\ \mathbb{0} & \mathbb{0} & Q_1^T & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ \mathbb{0} & \mathbb{0} & \mathbb{0} & \dots & Q_1^T & \mathbb{0} \\ \mathbb{0} & \mathbb{0} & \mathbb{0} & \dots & \mathbb{0} & I \end{bmatrix} \cdot \begin{bmatrix} B\underline{00} & \mathbb{0} & & \\ \underline{0}B\underline{0} & \mathbb{0} & & \\ \underline{00}B & \mathbb{0} & & \\ & \ddots & \ddots & \\ & \mathbb{0} & & \underline{0}B \\ & S_0 & & \end{bmatrix} =$$

$$\begin{bmatrix} R_1\underline{00} & \mathbb{0} & & \\ \underline{0}R_1\underline{0} & \mathbb{0} & & \\ \underline{00}R_1 & \mathbb{0} & & \\ & \ddots & \ddots & \\ & \mathbb{0} & & \underline{0}R_1 \\ & S_0 & & \end{bmatrix} = (S^*)^{(1)}.$$

Skinny QR factorization

2nd Step

$$\begin{bmatrix} R_1\underline{0} \\ \underline{0}R_1 \end{bmatrix} =: B_1 \text{ Apply QR factorization to } B_1\text{: } Q_2^T B_1 = R_2,$$

$$\begin{bmatrix} R_2\underline{00} & \mathbb{0} & & \\ \underline{00}R_2 & \mathbb{0} & & \\ & \ddots & \ddots & \\ & \mathbb{0} & & R_2 \\ & S_0 & & \\ & \mathbb{0} & & \underline{0}R_1 \end{bmatrix} = (S^*)^{(2)}.$$

Skinny QR factorization

r-th Step

Triangularize the two first same blocks B_{r-1} of $(S^*)^{(r)}$ using QR factorization $(Q_r^T B_{r-1} = R_r)$

Update the remaining blocks without making any other calculations.

If the number of the same blocks at step r is odd, place the last one after the S_0 block.

Final Step

Apply the QR factorization to the remaining non-zero part of $(S^*)^{(r)}$: $(Q_{r+1}^*)^T (S^*)^{(r)} = R$.

Algorithm AGCD through Modified Generalized Sylvester matrix

1. Define a threshold $t > 0$.
   Apply the SVD algorithm to S^* using the skinny QR factorization for the first phase of SVD.
   Define a basis M for the right "near nullspace" of the Sylvester matrix S^* as follows: $S^* = U\Sigma V^T$.
   The columns of V corresponding to the smaller than t singular values, define the right "near null space" of S^*.
2. Define the GCD Matrix Pencil $Z(s) = s \cdot M_1 - M_2$,where M_1 and M_2 are the matrices obtained from M by deleting the last and the first row of M respectively.
3. Form the polynomial matrix $Z(s)$ with elements all nonzero determinants of maximal order.
   Specify the matrix B containing the coefficients of the polynomials of $Z(s)$.
4. Find the SVD of B: $B = \widetilde{U} \cdot \widetilde{\Sigma}\widetilde{V}^T$.
   The corresponding to the largest singular value column of $\widetilde{V}$ defines the approximate GCD.

Bézout matrix

Definition

Let $f(x)$ and $g(x)$ be two polynomials:

$$f(x) = \sum_{l=0}^{n} u_l x^l = u_n x^n + u_{n-1} x^{n-1} + \ldots + u_2 x^2 + u_1 x + u_0$$

$$g(x) = \sum_{l=0}^{p} v_l x^l = v_p x^p + v_{p-1} x^{p-1} + \ldots + v_2 x^2 + v_1 x + v_0$$

$\deg\{f(x)\} = n$ *and* $\deg\{g(x)\} = p$, $n \geq p$ *and* $u_n, v_p \neq 0$. *Then, the Bézout matrix associated with the polynomials $f(x)$ and $g(x)$ is the following $n \times n$ symmetric matrix:*

$$B \triangleq B(f,g) = [b_{i,j}]_{i,j=1,\ldots,n} =$$

$$= \begin{bmatrix} u_1 & \cdots & u_n \\ \vdots & \iddots & \\ u_n & & 0 \end{bmatrix} \begin{bmatrix} v_0 & \cdots & v_{n-1} \\ & \ddots & \vdots \\ 0 & & v_0 \end{bmatrix} - \begin{bmatrix} v_1 & \cdots & v_n \\ \vdots & \iddots & \\ v_n & & 0 \end{bmatrix} \begin{bmatrix} u_0 & \cdots & u_{n-1} \\ & \ddots & \vdots \\ 0 & & u_0 \end{bmatrix} \quad (1)$$

Bézout matrix

The elements $b_{i,j}$ of the Bézout matrix are given by

$$b_{i,j} = |u_0\, v_{i+j-1}| + |u_1\, v_{i+j-2}| + \ldots + |u_l\, v_{i+j-l-1}| \tag{2}$$

where $l = \min(i-1, j-1)$, $u_r = v_r = 0$ if $r > n$
and $|u_r v_s| = u_s\, v_r - u_r\, v_s$.

Theorem

Let $f(x)$ and $g(x)$ be two polynomials as given in Definition 1. The greatest common divisor of the polynomials denoted by $\gcd(f, g)$, is a polynomial of degree $\deg\{\gcd(f, g)\} \leq p$ such that

$$\dim\{\mathit{NullSpace}\,(B(f, g))\} = \deg\{\gcd(f, g)\} = n - \mathit{rank}\,(B(f, g)) \tag{3}$$

Theorem

[Diaz-Toca and L. Gonzalez-Vega] 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*

ii) *every column c_i for $i = 1, 2, \ldots, k$ can be written as a linear combination of $c_{k+1}, \ldots, c_n$:*

$$c_{k-i} = \sum_{j=k+1}^{n} {h_{k-i}}^{(j)} c_j, \quad i = 0, 1, \ldots, k-1 \tag{4}$$

iii) *There are $d_1, d_2, \ldots, d_k$ such that $d_j = d_k \cdot h_{k-j+1}^{(k+1)}$ and $d_0 \neq 0$:*

$$\begin{bmatrix} d_k \\ d_{k-1} \\ d_{k-2} \\ \vdots \\ d_0 \end{bmatrix} = d_k \begin{bmatrix} 1 \\ h_k^{(k+1)} \\ h_{k-1}^{(k+1)} \\ \vdots \\ h_1^{(k+1)} \end{bmatrix} \tag{5}$$

The GCD of the polynomials f and g is

$$gcd(f,g) = d_0 s^k + d_1 s^{k-1} + \ldots + d_{k-1} s + d_k \tag{6}$$

Theorem

(QR factorization with column pivoting (QRCP) for rank deficient Bézout matrices)
Let $B \in \mathbb{R}^{n\times n}$ and $rank(B) = r < n$, where B is a Bézout matrix as defined previously. Then, there always exist a permutation matrix Π of order n and a $n \times n$ orthogonal matrix Q [Golub 1996] such that

$$Q^T B\Pi = R = \begin{bmatrix} R_{11} & R_{12} \\ 0 & 0 \end{bmatrix} \begin{matrix} r \\ n-r \end{matrix} \qquad (7)$$
$$\begin{matrix} r & n-r \end{matrix}$$

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

$$\widehat{b}_{c_k} = \sum_{i=1}^{\min\{r,k\}} r_{ik} q_i \in span\{q_1, \ldots, q_r\}, \quad k = 1, 2, \ldots, n \qquad (8)$$

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

Definition

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, $i = 1, \ldots, n$. Then the *generalized Bézout* matrix is defined as follows:

$$B = \begin{bmatrix} B_1 \\ B_2 \\ \vdots \\ B_n \end{bmatrix} \in \mathbb{R}^{mn \times n} \tag{9}$$

Remark

Theorems 2, 3, and 4 also hold for the generalized Bézout matrix.

Example: GCD through Bézout matrix

$$\mathcal{P}_{2,5} = \left\{ \begin{array}{rcl} p_1(s) & = & s^5 - 24s^4 + 208s^3 - 786s^2 + 1231s - 630 \\ p_2(s) & = & s^5 - 23s^4 + 195s^3 - 745s^2 + 1244s - 672 \end{array} \right\} \tag{10}$$

The exact GCD is $s^2 - 8s + 7$. The Bézout matrix of the given polynomials in the set $\mathcal{P}_{2,5}$ is

$$\begin{aligned} B = Bez\{p_1, p_2\} &= \begin{bmatrix} -1 & 13 & -41 & -13 & 42 \\ 13 & -145 & 185 & 1585 & -1638 \\ -41 & 185 & 3275 & -20345 & 16926 \\ -13 & 1585 & -20345 & 77615 & -58842 \\ 42 & -1638 & 16926 & -58842 & 43512 \end{bmatrix} \\ &= \begin{bmatrix} b_{c_1} & b_{c_2} & b_{c_3} & b_{c_4} & b_{c_5} \end{bmatrix} \end{aligned} \tag{11}$$

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

Example: GCD through Bézout matrix

Apply QRCP to B, such that

$$B\,\Pi = Q\,R \tag{12}$$

where

$$\begin{aligned} Q &= \begin{bmatrix} -0.0001306 & 0.017252 & 0.12062 & 0.52198 & -0.84421 \\ 0.015928 & -0.23579 & -0.85628 & -0.32276 & -0.32674 \\ -0.20444 & 0.83472 & 0.029962 & -0.44344 & -0.25281 \\ 0.77995 & -0.13851 & 0.31873 & -0.46068 & -0.24225 \\ -0.5913 & -0.47767 & 0.38697 & -0.46314 & -0.24074 \end{bmatrix} \\ &= \begin{bmatrix} q_1 & q_2 & q_3 & q_4 & q_5 \end{bmatrix} \end{aligned} \tag{13}$$

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

and

$$\Pi = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \tag{15}$$

Example: GCD through Bézout matrix

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

$$B_{perm} = \begin{bmatrix} -13 & -41 & 13 & 42 & -1 \\ 1585 & 185 & -145 & -1638 & 13 \\ -20345 & 3275 & 185 & 16926 & -41 \\ 77615 & -20345 & 1585 & -58842 & -13 \\ -58842 & 16926 & -1638 & 43512 & 42 \end{bmatrix} \tag{16}$$

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

QRCP indicates that $r = rank(B) = 3$ and $\deg\{\gcd(\mathcal{P}_{2,5})\} = 2$. From Theorem 3 we know that the last 3 columns of the initial Bézout matrix B in (11), i.e. b_{c_3}, 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_3}, b_{c_4} and b_{c_5}. Thus, from (4) in Theorem 3 we have:

$$b_{c_2} = h_2^{(3)} b_{c_3} + h_2^{(4)} b_{c_4} + h_2^{(5)} b_{c_5} \tag{17}$$

$$b_{c_1} = h_1^{(3)} b_{c_3} + h_1^{(4)} b_{c_4} + h_1^{(5)} b_{c_5} \tag{18}$$

Example: GCD through Bézout matrix

Let $d_0 s^2 + d_1 s + d_2$ 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 4, the columns q_1, q_2 and q_3 of Q generate the range of B_{perm}. From (8) we have:

$$\begin{aligned}
\widehat{b}_{c_1} &= b_{c_4} = R_{11}\, q_1 \\
\widehat{b}_{c_2} &= b_{c_3} = R_{12}\, q_1 + R_{22}\, q_2 \\
\widehat{b}_{c_3} &= c_{c_2} = R_{13}\, q_1 + R_{23}\, q_2 + R_{33}\, q_3 \\
\widehat{b}_{c_4} &= b_{c_5} = R_{14}\, q_1 + R_{24}\, q_2 + R_{34}\, q_3 \\
\widehat{b}_{c_5} &= b_{c_1} = R_{15}\, q_1 + R_{25}\, q_2 + R_{35}\, q_3
\end{aligned} \tag{19}$$

Example: GCD through Bézout matrix

Since the columns b_{c_2} and b_{c_1} of the initial Bézout matrix B correspond to $\widehat{b}_{c_3}$ and $\widehat{b}_{c_5}$ of the permuted Bézout matrix B_{perm}, respectively, we express $\widehat{b}_{c_3}$ and $\widehat{b}_{c_5}$ as linear combinations of $\widehat{b}_{c_1}$, $\widehat{b}_{c_2}$ and $\widehat{b}_{c_4}$. Since each q_i, $i = 1, 2, 3$ is given by an analytic formula as the solution of the lower triangular system, formed from the 1st, 2nd, and 4th equation of (19), substitute symbolically in the 3rd and 5th equation of (19) and obtain:

$$\widehat{b}_{c_3} = R_{13}\, q_1 + R_{23}\, q_2 + R_{33}\, q_3 \tag{20}$$

$$\widehat{b}_{c_5} = R_{15}\, q_1 + R_{25}\, q_2 + R_{35}\, q_3 \tag{21}$$

Example: GCD through Bézout matrix

Therefore,

$$\begin{aligned}\widehat{b}_{c_3} &= -1.14282712402397\,\widehat{b}_{c_2} - 1.16326188998929\,\widehat{b}_{c_1} - 1.16617476075485\,\widehat{b}_{c_4}\\ \widehat{b}_{c_5} &= 0.142855765690511\,\widehat{b}_{c_2} + 0.163268401615028\,\widehat{b}_{c_1} + 0.166183704498703\,\widehat{b}_{c_4}\end{aligned}$$

and from the correspondence of the columns of B and B_{perm}:

$$\begin{aligned}b_{c_2} = \widehat{b}_{c_3} &= -1.14282712402397\,b_{c_3} - 1.16326188998929\,b_{c_4} - 1.16617476075485\,b_{c_5}\\ b_{c_1} = \widehat{b}_{c_5} &= 0.142855765690511\,b_{c_3} + 0.163268401615028\,b_{c_4} + 0.166183704498703\,b_{c_5}\end{aligned}$$

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 $\mathcal{P}_{2,5}$. That is

$$gcd(\mathcal{P}_{2,5}) = 1.0\,s^2 - 7.999866988216918\,s + 7.000067481815496$$

Figure: Computational performance

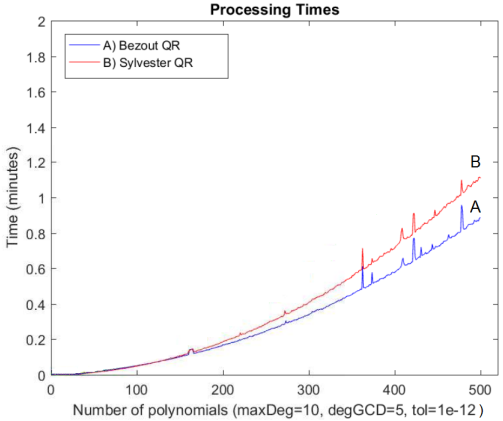
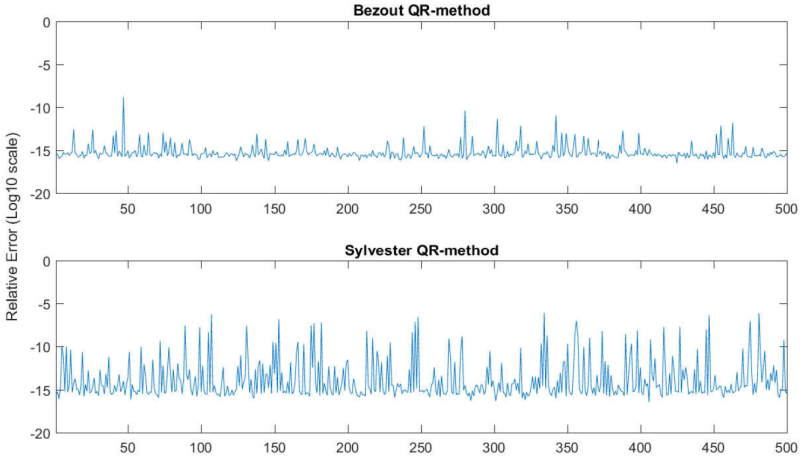


Figure: Numerical efficiency



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
		$n \simeq p$	$m \simeq n \simeq p$
Sylvester QR	$(n+p)^2\left((mn+p)-\frac{n+p}{3}\right)$	$4n^3\left(m+\frac{1}{3}\right)$	$4n^4$
Modified Sylvester QR	$(n+p)^3(2\log_2 n-\frac{1}{3})$	$4n^3\left(4\log_2 n+\frac{1}{3}\right)$	$4n^3\left(6\log_2 n+\frac{1}{3}\right)$
	$+(n+p)^2(2m\log_2 n+p)$	$+8n^2 m\log_2 n$	
Bézout QR	$2n^2(mn-\frac{n}{3})$	$2n^2(mn-\frac{n}{3})$	$2n^4$
Bézout QRCP	$2mn^2r-r^2(mn+n)+\frac{2r^3}{3}$	$2mn^2r-r^2(mn+n)+\frac{2r^3}{3}$	$2n^3r-n^2r^2$s

Conclusions

- For a large set of polynomials with high degree, the modified Sylvester QR method is more preferable.
- The Bézout QRCP exploits the rank deficiency of the matrices.

Future work

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.

References

1 T. Beelen and Van Dooren, P., A pencil approach for embedding a polynomial matrix into a unimodular matrix, SIAM J. Matrix Anal. Appl., 9, 1988, pp. 77-89.

2 D. A. Bini and P. Boito, A Fast Algorithm for Approximate Polynomial GCD Based on Structured Matrix Computations, Operator Theory: Advances and Applications, 199, 2010, pp. 155-173.

3 R. M. Corless and S. M. Watt and L. Zhi, QR Factoring to compute the GCD of Univariate Approximate Polynomials, IEEE Transactions on Signal Processing, 52, No. 12, 2004, pp. 3394-3402.

4 G. M. Diaz-Toca and L. Gonzalez-Vega, Barnetts theorems about the greatest common divisor of several univariate polynomials through Bezout-like matrices, J. Symbolic Computation, 34, 2002, pp.59-81.

5 Golub, G.H. and Van Loan, C.F., Matrix Computations, Third Edition, The John Hopkins Univercity Press, Baltimore, London, 1989.

6 N. Karcanias, Invariance properties and characterisation of the greatest common divisor of a set of polynomials, Int. J. Control, 46, 1987, pp. 1751-1760.

7 N. Karcanias and M. Mitrouli and D. Triantafyllou, Matrix Pencil methodologies for computing the greatest common divisor of polynomials: Hybrid algorithms and their performance, Int. Journ. of Control, 79, No. 11, 2006, pp. 1447-1461.

8 I. S. Pace and S. Barnett, Comparison of algorithms for calculation of g.c.d of polynomials, Int. J. Control, 4, No. 2, 1973, pp. 211-216.

9 T. Sasaki and M. Sasaki, Polynomial remainder sequence and approximate GCD, ACM SIGSAM Bull., 31, 1997, pp. 4-10.

10 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, 2011, pp. 1587-1603.

Thank you

for your Attention