CALCULATION OF THE GREATEST COMMON DIVISOR OF PERTURBED POLYNOMIALS

Jan Zítko, Ján Eliaš
Department of Numerical Mathematics,
Faculty of Mathematics and Physics, Charles University
Sokolovská 83, Prague 8, Czech Republic
zitko@karlin.mff.cuni.cz, janelias@ymail.com

Abstract
The coefficients of the greatest common divisor of two polynomials $f$ and $g$ (GCD($f$, $g$)) can be obtained from the Sylvester subresultant matrix $S_j(f, g)$ transformed to lower triangular form, where $1 \leq j \leq d$ and $d = \deg(\text{GCD}(f, g))$ needs to be computed. Firstly, it is supposed that the coefficients of polynomials are given exactly. Transformations of $S_j(f, g)$ for an arbitrary allowable $j$ are in details described and an algorithm for the calculation of the GCD($f$, $g$) is formulated. If inexact polynomials are given, then an approximate greatest common divisor (AGCD) is introduced. The considered techniques for an AGCD computations are shortly discussed and numerically compared in the presented paper.

1. Introduction
Consider the polynomials $f$ and $g$,
\begin{align*}
f(x) &= a_0x^m + a_1x^{m-1} + \cdots + a_{m-1}x + a_m, \quad a_0 \times a_m \neq 0, \quad (1) \\
g(x) &= b_0x^n + b_1x^{n-1} + \cdots + b_{n-1}x + b_n, \quad b_0 \times b_n \neq 0. \quad (2)
\end{align*}
In the first part of this paper it is assumed that the coefficients are given exactly, all calculations are performed symbolically and $m \geq n$. Let us put $f_0 := f$, $f_1 := g$. The polynomials
\begin{align*}
f_r(x) &= q_r(x)f_{r+1}(x) + f_{r+2}(x), \quad \deg(f_{r+2}) < \deg(f_{r+1}), \\
&\text{for } r = 0, 1, 2, \ldots, \quad f_r \neq 0 \forall r \leq k
\end{align*}
in the successive divisions of Euclid’s algorithm are well defined, $[1, 7, 15]$. If $f_{k+1} = 0$ then $f_k$ is the GCD of $f_0$ and $f_1$, which is written as $f_k = \text{GCD}(f_0, f_1) = \text{GCD}(f, g)$. 

215
The Sylvester matrix $S(f, g) \in \mathbb{R}^{(m+n) \times (m+n)}$, $[1, 3, 4, 7, 12, 13, 15]$, is the matrix

$$
S(f, g) = \begin{bmatrix}
0 & b_0 \\
a_0 & a_1 & b_1 & b_0 \\
\cdot & a_1 & \cdot & \cdot & b_1 \\
\cdot & \cdot & \cdot & a_0 & \cdot & \cdot & b_0 \\
a_m & \cdot & a_1 & b_n & \cdot & b_1 \\
\cdot & \cdot & \cdot & \cdot & \cdot & b_n & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
a_m & \cdot & \cdot & \cdot & \cdot & b_n \\
\end{bmatrix}
$$

Let $j$ be an integer, $1 \leq j \leq n$. The $j$th Sylvester subresultant matrix $S_j(f, g) \in \mathbb{R}^{(m+n-j+1) \times (m+n-2j+2)}$ is formed by deleting the last $(j-1)$ rows, and the last $(j-1)$ columns of the coefficients of $f$ and $g$ of $S(f, g)$. The vector $e_i$ denotes the $i$th column of the identity $r \times r$ matrix $I_r$, and the matrix $E_{i,j}(\sigma) = I_r - \sigma e_i e_j^T$, where $\sigma \in \mathbb{R}$, is the elementary triangular matrix. It is lower and upper triangular matrix for $i \geq j$ and $i \leq j$, respectively.

Transformations of the Sylvester subresultant matrix $S_j(f, g)$ that correspond to the first stage of Euclid’s algorithm can be expressed by multiplying $S_j(f, g)$ by the elementary triangular matrices. The polynomial $f_2$ arises from the first stage. For illustration, let us consider the Sylvester resultant matrix $S_2 := S_2(f, g)$ for the polynomials $f$ and $g$ of degrees $m = 6$ and $n = 3$.

The first step in the transformation of $S_2$ consists of the subtraction of the third and fourth column, multiplied by $\sigma_1 = a_0/b_0$, from the first and second column, respectively. This is implemented in such a way that the matrix $S_2$ is multiplied successively by the matrices $E_{3,1}(\sigma_1)$ and $E_{4,2}(\sigma_1)$ yielding $S_2^{(1)} := S_2 E_{3,1}(\sigma_1) E_{4,2}(\sigma_1)$,

$$
S_2^{(1)} = \begin{bmatrix}
0 & b_0 \\
a_1^{(1)} & 0 & b_1 & b_0 \\
a_2^{(1)} & a_1^{(1)} & b_2 & b_1 & b_0 \\
a_3^{(1)} & a_2^{(1)} & b_3 & b_2 & b_1 & b_0 \\
a_4^{(1)} & a_3^{(1)} & b_4 & b_3 & b_2 & b_1 \\
a_5^{(1)} & a_4^{(1)} & b_5 & b_4 & b_3 & b_2 \\
a_6^{(1)} & a_5^{(1)} & b_6 & b_5 & b_4 & b_3 \\
\end{bmatrix}
$$

where

$$
a_i^{(1)} = \begin{cases}
\frac{a_i - (a_0/b_0) b_i}{\sigma_1} & i = 1, 2, 3 \\
a_i & i = 4, 5, 6.
\end{cases}
$$

Analogously, the numbers $\sigma_2$, $\sigma_3$, and $\sigma_4$ can be constructed such that the first two columns of the matrix $S_2^{(4)}$, where successively

$$
S_2^{(2)} = S_2^{(1)} E_{4,1}(\sigma_2) E_{5,2}(\sigma_2), \quad S_2^{(3)} = S_2^{(2)} E_{5,1}(\sigma_3) E_{6,2}(\sigma_3), \quad S_2^{(4)} = S_2^{(3)} E_{6,1}(\sigma_4) E_{7,2}(\sigma_4),
$$

contain the elements $0, 0, 0, 0, a_4, a_5, a_6$ $^1$ at the locations of $0, a_4^{(1)}, a_4^{(1)}, a_4^{(1)}, a_4^{(1)}, a_5^{(1)}, a_6^{(1)}$ of $S_2^{(1)}$.

$^1$The upper index, e.g. $a_4^{(4)}$, specifies that the coefficients belong to the matrix $S_2^{(4)}$.

216
Then the permutation matrix \( P = [e_3, e_4, e_5, e_6, e_7, e_1, e_2] \in \mathbb{R}^{7 \times 7} \) applied to \( S_2^{(4)} \) gives

\[
S_2^{(4)} P = \begin{bmatrix}
    b_0 & 0 & 0 & 0 & 0 & 0 & 0 \\
    b_1 & b_0 & 0 & 0 & 0 & 0 & 0 \\
    b_2 & b_1 & b_0 & 0 & 0 & 0 & 0 \\
    b_3 & b_2 & b_1 & b_0 & 0 & 0 & 0 \\
    - & - & - & - & 0 & b_3 & b_2 \\
    0 & 0 & b_3 & b_2 & b_1 & b_0 & 0 \\
    0 & 0 & 0 & b_3 & b_2 & b_1 & b_0 \\
\end{bmatrix}
\]

\[
= \begin{bmatrix}
    L_{1,1} & 0 \\
    - & - \\
    L_{2,1} & L_{2,2} \\
\end{bmatrix}
\]

where \( L_{2,2} = S_2(g, f_2) \) and \( f_2(x) = a_4^{(4)} x^2 + a_5^{(4)} x + a_6^{(4)} \) is the first nonzero polynomial produced by Euclid’s algorithm if \( f_2 \neq 0 \). In this case the matrix \( L_{1,1} \) is square, lower triangular and nonsingular.

The following four cases may happen:

1. \( f_2 = 0 \), i.e. \( a_4^{(4)} = a_5^{(4)} = a_6^{(4)} = 0 \). Then \( g \) divides \( f \) and the matrix \( S_2^{(4)} P \) without any block structure is lower triangular matrix having two last zero columns.

2. \( a_4^{(4)} \neq 0 \) and \( f_2 \) divides \( g \). Then elementary matrices applied to \( L_{2,2} \) transform \( L_{2,2} \) to the matrix \( S_2^{(4)} \).

   Hence, the matrices \( S_2^{(4)} \) and \( S_2 \) are rank deficient of order 1. In this case \( n_2 := \deg(\text{GCD}(f, g)) = 2 \).

3. \( a_4^{(4)} \neq 0 \) and \( f_2 \) does not divide \( g \). Then elementary matrices applied to \( L_{2,2} \) transform \( L_{2,2} \) to the lower triangular matrix having linearly independent columns.

4. \( a_4^{(4)} = 0 \) but \( f_2 \neq 0 \). Then the matrix \( S_2^{(4)}(f, g) \) can be transformed into the form

\[
\tilde{S}_2^{(4)} = \begin{bmatrix}
    b_0 & 0 & 0 & 0 & 0 & 0 & 0 \\
    b_1 & b_0 & 0 & 0 & 0 & 0 & 0 \\
    b_2 & b_1 & b_0 & 0 & 0 & 0 & 0 \\
    b_3 & b_2 & b_1 & b_0 & 0 & 0 & 0 \\
    - & - & - & - & 0 & b_3 & b_2 \\
    0 & 0 & b_3 & b_2 & b_1 & b_0 & 0 \\
    0 & 0 & 0 & b_3 & b_2 & b_1 & b_0 \\
\end{bmatrix}
\]

and no other polynomials can be calculated in Euclid’s algorithm in the last two cases. The matrices \( S_2^{(4)}(f, g) \) and \( S_2 \) have full column rank.

217
In general, if the Sylvester subresultant \( S_j(f, g) \) has full column rank, we have to go back to \( S_{j-1}(f, g), S_{j-2}(f, g), \ldots \) as long as the rank deficient matrix appears. If \( S_1(f, g) = S(f, g) \) has full column rank, then \( f \) and \( g \) are coprime. Just presented example is generalized in the following section. The results are original.

2. Matrix formulation for the transformation of the Sylvester subresultant matrix

Let us denote \( f_0 := f \) and \( f_1 := g \), where \( f \) and \( g \) are defined in (1) and (2), respectively. Denote \( n_0 := m = \deg(f_0), n_1 := n = \deg(f_1). \)

Let us assume that the matrices \( S_j(f_0, f_1), S_j(f_1, f_2), \ldots \) can be constructed by Euclid’s algorithm for an index \( j \). According to our previous example, the following theorem can be easily seen. Let us write shortly \( S_j := S_j(f_0, f_1). \)

**Theorem 1.** Let \( f_0 \) and \( f_1 \) be polynomials of degrees \( n_0 \) and \( n_1 \), respectively, \( n_0 \geq n_1 \geq 1. \) It is assumed that Euclid’s algorithm yields the polynomials \( f_2, f_3, \ldots, f_k, f_{k+1} = 0 \) of degrees \( n_2, n_3, \ldots, n_k \). Therefore \( f_k = \text{GCD}(f_0, f_1) \). Denote \( d := n_k \) and 
\[
\begin{align*}
\quad v_d(x) &= v_0 x^d + v_1 x^{d-1} + \cdots + v_{d-1} x + v_d.
\end{align*}
\]
Consider an integer \( j \in \{1, 2, \ldots, n\} \). Then the following statements hold:

1) There exists a nonsingular matrix \( Q_j \) of order \( n_0 + n_1 - 2j + 2 \) such that the matrix \( S_j Q_j \) has the following block structure. We distinguish two cases:

a) If \( j \leq d \), then

\[
S_j Q_j = \begin{bmatrix}
L_{1,1} & 0 \\
-1 & -1 \\
L_{2,1} & L_{2,2}
\end{bmatrix},
\]

where \( L_{1,1} \) is a square lower triangular matrix with non-zero diagonal elements and \( L_{2,2} \) is a rectangular matrix with \( (n_{k-1} + n_k - 2j + 2) \) columns if \( f_2 \neq 0 \). Contrariwise if \( f_2 = 0 \) then \( g \) divides \( f \) and the matrix \( S_j Q_j \) is lower triangular matrix having last \( n_1 - j + 1 \) zero columns. In the following let \( f_2 \neq 0 \). Then the matrix \( L_{2,2} \) has the following form:

\[
\begin{align*}
(i) \text{ case when } j \leq d & \\
L_{2,2} = & \begin{bmatrix}
v_0 & 0 & 0 \\
v_1 & 0 & 0 \\
\vdots & \ddots & \vdots \\
v_d & v_0 & 0 \\
\vdots & v_1 & 0 \\
v_d & \vdots & 0 \\
v_d & \vdots & \vdots \\
v_d & \vdots & 0 \\
\end{bmatrix}_n \\
\end{align*}
\]

\[
\begin{align*}
(ii) \text{ special case when } j = d & \\
L_{2,2} = & \begin{bmatrix}
v_0 & 0 & 0 \\
v_1 & v_0 & 0 \\
\vdots & \ddots & \vdots \\
v_d & v_0 & 0 \\
\vdots & v_1 & 0 \\
v_d & \vdots & 0 \\
v_d & \vdots & \vdots \\
v_d & \vdots & 0 \\
\end{bmatrix}_n \\
\end{align*}
\]

The number of columns of the last two matrices is \( (n_{k-1} - n_k + 1) \).
Moreover, the presented scheme of matrices (i) and (ii) shows that
\[
\text{rank}(S_j) = \text{rank}(Q_j S_j) = n_0 + n_1 - 2(j - 1) - (n_k - j + 1) = n_0 + n_1 - j - n_k + 1
\]
and the nonzero columns of the matrix \(L_{2,2}\) contain the coefficients of the polynomial \(f_k\). In case \(j = d = n_k\), the matrix \(S_d\) is rank deficient of order 1.

b) If \(j > d\), then \(S_j Q_j\) is a lower triangular matrix with linearly independent columns. Hence, \(S_j Q_j\) and therefore \(S_j\) has full column rank.

2) If \(n_k = 0\), then the matrix \(S_1(f_0, f_1)\) having full rank \(n_0 + n_1\) is only considered, \(f_k = v_0 \neq 0\) and \(L_{2,2} = v_0 I_{n_k-1}\).

3) The next equivalences follow from the statements formulated above:
\[
\begin{align*}
\text{rank}(S_d(f_0, f_1)) &= n_0 + n_1 - 2d + 1 \iff \deg(\text{GCD}(f_0, f_1)) = d, \\
\text{rank}(S_j(f_0, f_1)) &= n_0 + n_1 - 2j + 1 \iff \deg(\text{GCD}(f_0, f_1)) > j.
\end{align*}
\]

Just presented overview shows the relation between the \(\text{rank}(S_j)\) and the degree of \(\text{GCD}(f_0, f_1)\). Hence if the polynomials \(f_0\) and \(f_1\) are known exactly and the computations are performed symbolically, then the transformation of the Sylvester subresultant matrix \(S_j(f_0, f_1), j \leq d\), to the lower triangular form with the resultant matrix \(L_{2,2}\) yields the coefficients of the \(\text{GCD}(f_0, f_1)\).

3. Calculation of GCD
Consider the polynomials \(f\) and \(g\) in (1) and (2) of degrees \(m = \deg(f_0)\) and \(n = \deg(f_1)\), and put \(f_0 = f\) and \(f_1 = g\). Let \(h\) be the exact \(\text{GCD}(f_0, f_1)\) with \(d = \deg(h)\). There exist two polynomials \(w_0\) and \(w_1\) so that
\[
f_i = h w_i \quad \text{for} \quad i = 0, 1, \quad \text{where} \quad \deg(w_0) = m - d, \quad \deg(w_1) = n - d.
\]
Hence \(f_0/w_0 = f_1/w_1 \Rightarrow f_0 w_1 - f_1 w_0 = 0\). Using Cauchy matrices, we can rewrite the last equality in the form
\[
C_{n-d+1}(f_0) \vec{w}_1 - C_{m-d+1}(f_1) \vec{w}_0 = \left[ C_{n-d+1}(f_0), C_{m-d+1}(f_1) \right]_{S_d} \begin{bmatrix} \vec{w}_1 \\ -\vec{w}_0 \end{bmatrix} = \vec{0}, \quad (3)
\]
where the vectors of coefficients of the polynomials \(w_1, w_0\) are denoted by \(\vec{w}_1\) and \(\vec{w}_0\). The matrix \(S_d = [C_{n-d+1}, C_{m-d+1}] \in \mathbb{R}^{(m+n-d+1)(m+n-2d+2)}\) is rank deficient of order 1. The solution of (3) is the right singular vector corresponding to \(\sigma_{\min}(S_d(f_0, f_1))\) and can be computed by the Gauss-Newton iteration, see for example [2, 3, 8]. The coefficients of \(h\) are calculated as the least square solution of the equation
\[
C_{d+1}(w_1) \vec{h} = \vec{f}_1 \quad \text{or} \quad C_{d+1}(w_0) \vec{h} = \vec{f}_0.
\]
The smallest singular values

\[ \log_{10} \sigma_{\text{min}}(S_i) \]

Singular values of \( S_i \), \( i = 1, 2, \ldots, 10 \)

Figure 1: In the following graphs the smallest singular values of the Sylvester subresultant matrices \( S_9, S_8, S_7 \) and \( S_6 \), left-hand side, and the singular values of \( S_7 \), right-hand side, are drawn.

Let us demonstrate the mentioned theory on the following polynomials

\[ f_0(x) = (x - 1.2)^4(x + 2)^3(x - 0.5)^4, \quad f_1(x) = (x - 1.4)^2(x + 2)^3(x - 0.5)^4 \]

of degrees \( \deg(f_0) = 13 \) and \( \deg(f_1) = 9 \). Their GCD is the polynomial \( \text{GCD}(f_0, f_1) = h(x) = (x + 2)^3(x - 0.5)^4 = x^7 + 4x^6 + 1.5x^5 - 7.5x^4 - 0.9375x^3 + 6.375x^2 - 3.25x + 0.5 \)

of degree \( \deg(h) = d = 7 \). Theorem 1 says that \( S_7 \) is the first rank deficient matrix in the sequence \( S_9, S_8, S_7 \). For illustration see Figure 1.

The matrix \( S_7 \) is the first rank deficient matrix with the smallest singular value \( 7.1678_{10}^{-14} \) and the corresponding right singular vector

\[ [-0.1090, 0.3051, -0.2135, 0.1090, -0.0872, -0.7147, 0.9204, 0.9790, -2.1086, 0.9037]^T. \]

The LS solution of \( C_8(\vec{w}_0)\vec{h} = \vec{f}_1 \) yields the coefficients of the GCD \( \text{GCD}(f_0, f_1) = \vec{h} = [1, 4, 1.5, -7, 5, -0.9375, 6.375, -3.25, 0.5]^T \). The LS solution of the system \( C_8(-\vec{w}_0)\vec{h} = \vec{f}_0 \) yields the same vector \( \vec{h} = [1, 4, 1.5, -7, 5, -0.9375, 6.375, -3.25, 0.5]^T \).

4. **Approximate greatest common divisor**

It was assumed that the coefficients of polynomials are given exactly and the calculations are performed symbolically. But the calculation of the GCD is unstable in a computer environment and cannot be almost used. Moreover, numerical computation of the GCD is an ill-posed problem. Therefore the concept of an approximate greatest common divisor (AGCD) was introduced [3, 6, 13, 14].

**Definition.** Let \( f \) and \( g \) be two polynomials of degrees \( m \) and \( n \), respectively, and let \( 0 < \theta << 1 \) be a positive number. The degree of an approximate greatest common divisor with respect to \( \theta \) is the maximum integer \( j \leq \min(m, n) \) for which there exist polynomials \( \delta f \) and \( \delta g \) with \( \max(\| \delta f \|, \| \delta g \|) \leq \theta \) and \( \deg(\text{GCD}(f + \delta f, g + \delta g)) = j \). The approximate greatest common divisor denoted by \( \text{AGCD}(f, g) \) is defined by \( \text{AGCD}(f, g) = \text{GCD}(f + \delta f, g + \delta g) \).
Algorithms for the calculation of $\delta f$ and $\delta g$ are well known. However they are out of scope of this paper and cannot be analysed in this paper. Let us only mention the Structured Total Least Norm (STLN) method (see, for example, [10, 5, 13]) for the construction of a structured low rank approximation of the full rank Sylvester matrix in the AGCD approach.

For demonstration, let us again consider the polynomials from Section 3 and let us denote them by $\hat{f}$ and $\hat{g}$. Their exact GCD is the polynomial

$$\text{GCD}(\hat{f}, \hat{g}) = x^7 + 4x^6 + 1.5x^5 + 7.5x^4 - 0.9375x^3 + 6.375x^2 - 3.25x + 0.5.$$  

Let $f$ and $g$ be inexact forms of $\hat{f}$ and $\hat{g}$, i.e. the polynomials $\hat{f}$ and $\hat{g}$ with a noise expressed by a signal-to-noise ratio equal to $10^6$ added to their coefficients. The polynomials that arise from the application of the STLN method are denoted by $\tilde{f}$ and $\tilde{g}$. The schema of this process is as follows.

\[
\begin{align*}
\{ \hat{f}(x), \hat{g}(x) \} \quad &\text{perturbation} \quad \rightarrow \quad \{ f(x), g(x) \} \quad &\text{STLN} \quad \rightarrow \quad \{ \tilde{f}(x), \tilde{g}(x) \}
\end{align*}
\]

The polynomials $f$ and $g$ are theoretically coprime and the procedure that follows from Theorem 1 fails in the presence of greater noise. However, we can see from the table below that the coefficients of $\text{GCD}(\hat{f}, \hat{g})$ and $\text{GCD}(\tilde{f}, \tilde{g})$ of the polynomials computed by STLN are almost identical.

<table>
<thead>
<tr>
<th></th>
<th>$\text{GCD}(f, g)$</th>
<th>$\text{GCD}(\tilde{f}, \tilde{g})$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x^7$</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$x^6$</td>
<td>4</td>
<td>3.999978</td>
</tr>
<tr>
<td>$x^5$</td>
<td>1.5</td>
<td>1.499947</td>
</tr>
<tr>
<td>$x^4$</td>
<td>-7.5</td>
<td>-7.500006</td>
</tr>
<tr>
<td>$x^3$</td>
<td>-0.9375</td>
<td>-0.937463</td>
</tr>
<tr>
<td>$x^2$</td>
<td>6.375</td>
<td>6.375001</td>
</tr>
<tr>
<td>$x^1$</td>
<td>-3.25</td>
<td>-3.250011</td>
</tr>
<tr>
<td>$x^0$</td>
<td>0.5</td>
<td>0.499999</td>
</tr>
</tbody>
</table>

Acknowledgements

This work was supported by the grant prvouk p47. The authors thank for this support.

References


