

Jan Zítko; Ján Eliaš

Calculation of the greatest common divisor of perturbed polynomials

In: Jan Chleboun and Karel Segeth and Jakub Šístek and Tomáš Vejchodský (eds.): Programs and Algorithms of Numerical Mathematics, Proceedings of Seminar. Dolní Maxov, June 3-8, 2012. Institute of Mathematics AS CR, Prague, 2013. pp. 215–222.

Persistent URL: <http://dml.cz/dmlcz/702730>

Terms of use:

© Institute of Mathematics AS CR, 2013

Institute of Mathematics of the Czech Academy of Sciences provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.



This document has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library*
<http://dml.cz>

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 ($\text{GCD}(f, g)$) 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 $\text{GCD}(f, g)$ 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 ,

$$f(x) = a_0x^m + a_1x^{m-1} + \dots + a_{m-1}x + a_m, \quad a_0 \times a_m \neq 0, \quad (1)$$

$$g(x) = b_0x^n + b_1x^{n-1} + \dots + b_{n-1}x + b_n, \quad b_0 \times b_n \neq 0. \quad (2)$$

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

$$f_r(x) = q_r(x)f_{r+1}(x) + f_{r+2}(x), \quad \deg(f_{r+2}) < \deg(f_{r+1}),$$

for $r = 0, 1, 2, \dots$, $f_r \neq 0 \forall r \leq k$

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 $f_k = \text{GCD}(f_0, f_1) = \text{GCD}(f, g)$.

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

$$S_2^{(4)}P = \left[\begin{array}{cccc|ccc} b_0 & & & & 0 & 0 & 0 \\ b_1 & b_0 & & & 0 & 0 & 0 \\ b_2 & b_1 & b_0 & & 0 & 0 & 0 \\ b_3 & b_2 & b_1 & b_0 & 0 & 0 & 0 \\ - & - & - & - & + & - & - \\ 0 & b_3 & b_2 & b_1 & b_0 & a_4^{(4)} & 0 \\ 0 & 0 & b_3 & b_2 & b_1 & a_5^{(4)} & a_4^{(4)} \\ 0 & 0 & 0 & b_3 & b_2 & a_6^{(4)} & a_5^{(4)} \\ 0 & 0 & 0 & 0 & b_3 & 0 & a_6^{(4)} \end{array} \right] = \left[\begin{array}{c|c} L_{1,1} & 0 \\ - & + \\ L_{2,1} & L_{2,2} \end{array} \right]$$

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 $S_{2,\star}^{(4)}$.

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

$$S_{2,\star}^{(4)} = \begin{bmatrix} a_4^{(4)} & 0 & 0 \\ a_5^{(4)} & a_4^{(4)} & 0 \\ a_6^{(4)} & a_5^{(4)} & 0 \\ 0 & a_6^{(4)} & 0 \end{bmatrix}$$

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

$$\tilde{S}_2^{(4)} = \left[\begin{array}{cccc|ccc} b_0 & & & & 0 & 0 & \\ b_1 & b_0 & & & 0 & 0 & \\ b_2 & b_1 & b_0 & & 0 & 0 & \\ b_3 & b_2 & b_1 & b_0 & 0 & 0 & \\ - & - & - & - & + & - & - \\ 0 & b_3 & b_2 & b_1 & b_0 & 0 & 0 \\ 0 & 0 & b_3 & b_2 & b_1 & a_5^{(4)} & 0 \\ 0 & 0 & 0 & b_3 & b_2 & a_6^{(4)} & a_5^{(4)} \\ 0 & 0 & 0 & 0 & b_3 & 0 & a_6^{(4)} \end{array} \right]$$

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.

In general, if the Sylvester subresultant $S_j(f, g)$ has full column rank, we have to go back to $S_{j-1}(f, g), S_{j-2}(f, g), \dots$ 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 $S_j(f_0, f_1), S_j(f_1, f_2), \dots$ 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 $f_2, f_3, \dots, f_k, f_{k+1} = 0$ of degrees n_2, n_3, \dots, n_k . Therefore $f_k = \text{GCD}(f_0, f_1)$. Denote $d := n_k$ and $f_k(x) = v_0x^d + v_1x^{d-1} + \dots + v_{d-1}x + v_d$. Consider an integer $j \in \{1, 2, \dots, n\}$. 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_jQ_j has the following block structure. We distinguish two cases:*
 - a) *If $j \leq d$, then*

$$S_jQ_j = \left[\begin{array}{c|c} L_{1,1} & 0 \\ \hline - & - \\ L_{2,1} & L_{2,2} \end{array} \right],$$

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_jQ_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:

(i) case when $j \leq d$

$$L_{2,2} = \left[\begin{array}{cccc|ccc} v_0 & & & & 0 & \cdot & 0 \\ v_1 & v_0 & & & 0 & \cdot & 0 \\ \cdot & v_1 & \cdot & & 0 & \cdot & 0 \\ v_d & \cdot & \cdot & v_0 & 0 & \cdot & 0 \\ & v_d & \cdot & v_1 & 0 & \cdot & 0 \\ & & \cdot & \cdot & 0 & \cdot & 0 \\ & & & v_d & 0 & \cdot & 0 \end{array} \right]$$

$\underbrace{\hspace{10em}}_{n_{k-1} - j + 1}$
 $\underbrace{\hspace{10em}}_{n_k - j + 1}$

(ii) special case when $j = d$

$$L_{2,2} = \left[\begin{array}{cccc|ccc} v_0 & & & & 0 & & \\ v_1 & v_0 & & & 0 & & \\ \cdot & v_1 & \cdot & & 0 & & \\ v_d & \cdot & \cdot & v_0 & 0 & & \\ & v_d & \cdot & v_1 & 0 & & \\ & & \cdot & \cdot & 0 & & \\ & & & v_d & 0 & & \end{array} \right]$$

$\underbrace{\hspace{10em}}_{n_{k-1} - n_k + 1}$
 $\underbrace{\hspace{10em}}_1$

Moreover, the presented scheme of matrices (i) and (ii) shows that

$$\begin{aligned} \text{rank}(S_j) &= \text{rank}(Q_j S_j) = n_0 + n_1 - 2(j-1) - (n_k - j + 1) \\ &= n_0 + n_1 - j - n_k + 1 \end{aligned}$$

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:

$$\begin{aligned} \text{rank}(S_d(f_0, f_1)) &= n_0 + n_1 - 2d + 1 \Leftrightarrow \deg(\text{GCD}(f_0, f_1)) = d, \\ \text{rank}(S_j(f_0, f_1)) &< n_0 + n_1 - 2j + 1 \Leftrightarrow \deg(\text{GCD}(f_0, f_1)) > j. \end{aligned}$$

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

$$f_i = h w_i \text{ for } i = 0, 1, \quad \text{where } \deg(w_0) = m - d, \quad \deg(w_1) = n - d.$$

Hence $h = f_0/w_0 = f_1/w_1 \Rightarrow f_0 w_1 - f_1 w_0 = 0$. Using Cauchy matrices, we can rewrite the last equality in the form

$$C_{n-d+1}(f_0) \vec{w}_1 - C_{m-d+1}(f_1) \vec{w}_0 = \underbrace{[C_{n-d+1}(f_0), C_{m-d+1}(f_1)]}_{S_d} \begin{bmatrix} \vec{w}_1 \\ -\vec{w}_0 \end{bmatrix} = \vec{0}, \quad (3)$$

where the vectors of coefficients of the polynomials w_1, w_0 are denoted by \vec{w}_1 and \vec{w}_0 . The matrix $S_d = [C_{n-d+1}, C_{m-d+1}] \in \mathbb{R}^{(m+n-d+1) \times (m+n-2d+2)}$ 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

$$C_{d+1}(w_1) \vec{h} = \vec{f}_1 \quad \text{or} \quad C_{d+1}(w_0) \vec{h} = \vec{f}_0.$$

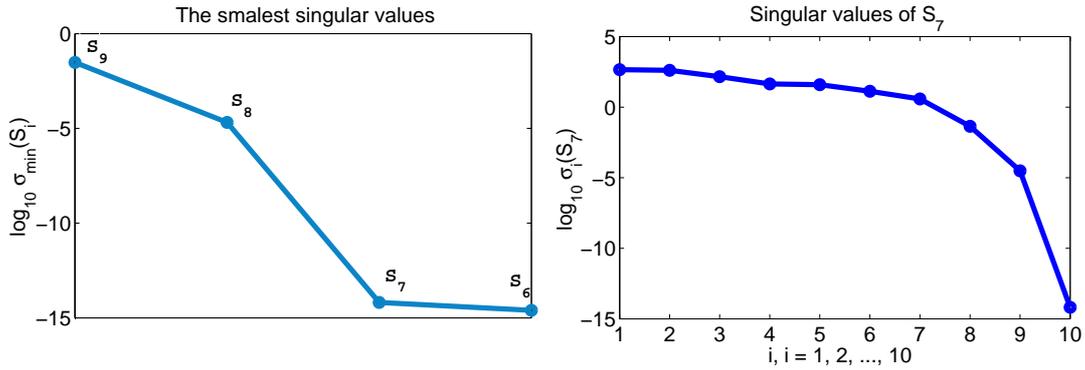


Figure 1: In the following graphs the smallest singular values of the Sylvester subresultant matrices S_9, S_8, S_7 and S_6 , left-hand side, and the singular values of S_7 , right-hand side, are drawn.

Let us demonstrate the mentioned theory on the following polynomials

$$f_0(x) = (x - 1.2)^4(x + 2)^5(x - 0.5)^4, \quad f_1(x) = (x - 1.4)^2(x + 2)^3(x - 0.5)^4 \quad (4)$$

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 $C_8(\vec{w}_1)\vec{h} = \vec{f}_1$ yields the coefficients of the $\text{GCD}(f_0, f_1) = \vec{h} = [1, 4, 1.5, -7, 5, -0.9375, 6.375, -3.25, 0.5]^T$. 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 $0 < \theta \ll 1$ be a positive number. The degree of an approximate greatest common divisor with respect to θ is the maximum integer $j \leq \min(m, n)$ for which there exist polynomials δf and δg 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 δf and δg 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.

$$\left\{ \begin{array}{l} \hat{f}(x) \\ \hat{g}(x) \end{array} \right\} \xrightarrow{\text{perturbation}} \left\{ \begin{array}{l} f(x) \\ g(x) \end{array} \right\} \xrightarrow{\text{STLN}} \left\{ \begin{array}{l} \tilde{f}(x) \\ \tilde{g}(x) \end{array} \right\}$$

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.

	$\text{GCD}(\hat{f}, \hat{g})$	$\text{GCD}(\tilde{f}, \tilde{g})$
x^7	1	1
x^6	4	3.999978
x^5	1.5	1.499947
x^4	-7.5	-7.500006
x^3	-0.9375	-0.937463
x^2	6.375	6.375001
x^1	-3.25	-3.250011
x^0	0.5	0.499999

Acknowledgements

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

References

- [1] Barnett, S.: *Polynomials and linear control systems*. Marcel Dekker, INC., New York and Basel, 1983.
- [2] Björk, Å.: *Numerical method for least square problems*. SIAM, Philadelphia, 1996.

- [3] Corless, R. M., Gianni, P. M., Trager, B. M., and Watt, S. M.: The singular value decomposition for polynomial systems. In: *Proc. ISSAC 95*, pp. 195–20. ACM Press 1995.
- [4] Eliaš, J.: *Problémy spojené s výpočtem největšího společného dělitele*. Bachelor thesis, Charles University, Faculty of Mathematics and Physics, 2009.
- [5] Kaltofen, E., Yang, Z., and Zhi, L.: Structured low rank approximation of Sylvester matrix. Preprint, 2005.
- [6] Kuřátko, J.: *Analysis of computing the greatest common divisors of polynomials*. Master thesis, Charles University, Faculty of Mathematics and Physics, 2012.
- [7] Leidacker, M. A.: Another theorem relating Sylvester’s matrix and the greatest common divisor. *Mathematics Magazine* **42**, No 3, (1969), pp. 126–128.
- [8] Li, T. Y. and Zeng, Z.: A rank-revealing method with updating, downdating and applications. *SIAM J. Matrix Anal. Appl.* **26** (4) (2005), 918–946.
- [9] Lee, T. L., Li, T. Y., and Zeng, Z.: A rank-revealing method with updating, downdating and applications. Part II. *SIAM J. Matrix Anal. Appl.* **31** (2) (2009), 503–525.
- [10] Rosen, J. B., Park, H., and Glick, J.: Total least norm formulation and solution for structured problems. *SIAM J. on Matrix Anal. Appl.* **17** (1) (1996), 110–128.
- [11] Saad, Y.: *Numerical methods for large eigenvalue problems*. Halstead Press, New York, 1992.
- [12] Winkler, J. R. and Zítko, J.: Some questions associated with the calculation of the GCD of two univariate polynomials. In: *Winter School and SNA’07*, pp. 130–137. Ostrava, 2007.
- [13] Winkler, J. R., and Allan, J. D.: Structured total least norm and approximate GCDs of inexact polynomials. *J. Comput. Appl. Math.* **215** (2006), 1–13.
- [14] Zeng, Z.: The approximate GCD of inexact polynomials, Part I: univariate algorithm. Preprint, 2004.
- [15] Zítko, J. and Eliaš, J.: Application of the rank revealing algorithm for the calculation of the GCD. In: *Winter School and SNA’12*, pp. 175–180. Liberec, 2012.