The transformation of the Sylvester matrix and the calculation of the GCD of two inexact polynomials

Joab R. Winkler⁽¹⁾, Jan Zítko⁽²⁾

 (1) The University of Sheffield, Department of Computer Science, Regent Court, 211 Portobello Street, Sheffield S1 4DP,
 United Kingdom
 (2) Charles University, Faculty of Mathematics and Physics,
 Department of Numerical Mathematics, Prague

Dolní Maxov 1. - 6. června 2008

Overview :

- 1. Introduction to problem
- 2. Transformation of the Sylvester matrix
- 3. A low rank approximation of the Sylvester matrix
- 4. The optimal value of the scale factor

1. Introduction

The determination of GCD of two polynomials arises in several applications.

An example of application: A common problem in linear systems theory is approximate pole-zero cancellation which reduces to the computation of an approximate GCD of two inexact polynomials. In particular, if a rational transfer function is given by

$$h(x) = rac{f(x)}{g(x)}$$

where f(x) and g(x) are polynomials, then it may be necessary to cancel out approximately equal factors of f(x) and g(x).

- the determination of almost common factors [Zarowski, Ma, Fairman]

[Euclid's algorithm is used for <u>exact</u> computation]

Euclid's algorithm $\overleftarrow{\leftarrow -- \rightarrow}$ the Sylvester matrix The polynomials f=f(x) and g=g(x)

$$egin{aligned} f(x) &= a_0 x^m + a_1 x^{m-1} + \dots + a_{m-1} x + a_m, \ g(x) &= b_0 x^n + b_1 x^{n-1} + \dots + b_{n-1} x + b_n, \ a_0 imes a_m
eq 0, \qquad b_0 imes b_n
eq 0. \end{aligned}$$

It is assumed $m \geq n$.

The Sylvester matrix $S(f,g) \in \mathbb{C}^{(m+n) imes (m+n)}$



The kth Sylvester submatrix $S_k \in \mathbb{C}^{(m+n-k+1) imes (m+n-2k+2)}$

[will be used later] is formed by deleting the last (k-1) rows,

and the last (k-1) columns of the coefficients of f(x)and g(x), of S(f,g).

We need the following notation:

The vector e_i denotes the ith column of the identity matrix I, and the matrix

 $E_{i,j}(\sigma) = I - \sigma e_i e_j^T$

where $\sigma \in \mathbb{C}$, is an *elementary triangular matrix*. It is lower and upper triangular for $i \geq j$ and $i \leq j$, respectively.

2. Transformation of the Sylvester matrix
Let
$$f_0 = f$$
 and $f_1 = g$,
 $f_i(x) = q_i(x)f_{i+1}(x) + f_{i+2}(x), \quad i = 0, 1, 2, ...$

- deg $f_{i+2} <$ deg f_{i+1} .
- If $f_k = 0$, then $f_{k-1} = \mathsf{GCD}\ (f,g)$.

The GCD(f,g) can be obtained by rearrangement of the Sylvester matrix S(f,g).

The special case m = 5 and n = 2 is considered.

To transformation S(f,g) into the triangular form;

$$(1) \qquad S(f,g) = egin{bmatrix} a_0 & b_0 \ a_1 & a_0 & b_1 & b_0 \ a_2 & a_1 & b_2 & b_1 & b_0 \ a_3 & a_2 & b_2 & b_1 & b_0 \ a_4 & a_3 & b_2 & b_1 & b_0 \ a_5 & a_4 & b_2 & b_1 \ a_5 & b_2 & b_1 \ b_2 & b_2 \ b_2 \ b_2 & b_2 \ b_2 \ b_2 & b_2 \ b_2 & b_2 \ b_2 \ b_2 & b_2 \ b_2$$

The first step ... the matrix (1) is postmultiplied successively by the matrices $E_{3,1}(a_0/b_0)$ and $E_{4,2}(a_0/b_0)$. This yields the matrix

•

$$(2) \quad S^{(1)}(f,g) = \begin{bmatrix} 0 & b_0 & & & \\ a_1^{(1)} & 0 & b_1 & b_0 & & \\ a_2^{(1)} & a_1^{(1)} & b_2 & b_1 & b_0 & & \\ a_3^{(1)} & a_2^{(1)} & & b_2 & b_1 & b_0 & \\ a_4^{(1)} & a_3^{(1)} & & b_2 & b_1 & b_0 & \\ a_5^{(1)} & a_4^{(1)} & & b_2 & b_1 & \\ & a_5^{(1)} & & & b_2 & b_1 \end{bmatrix}$$

-the corresponding polynomial operation has the form

$$egin{aligned} h_4(x):&=a_1^{(1)}x^4+a_2^{(1)}x^3+a_3^{(1)}x^2+a_4^{(1)}x+a_5^{(1)}\ &=f(x)-g(x)(a_0/b_0)x^3. \end{aligned}$$

The next step: the first nonzero element in the sequence $a_1^{(1)}$, $a_2^{(1)}$, $a_3^{(1)}$ is found - say $a_2^{(1)} \neq 0$, and the next step is the subtraction of the fifth and sixth columns, multiplied by $a_2^{(1)}/b_0$ from the first and second columns respectively. We have $a_1^{(1)} = 0$ and $h_4(x) = h_3(x) := a_2^{(1)}x^3 + a_3^{(1)}x^2 + a_4^{(1)}x + a_5^{(1)}$. In this case the matrix (2) is postmultiplied successively

by the matrices $E_{5,1}(a_2^{(1)}/b_0)$ and $E_{6,2}(a_2^{(1)}/b_0).$ This yields the matrix

$$(3) \quad S^{(2)}(f,g) = \begin{bmatrix} 0 & b_0 & & \\ 0 & 0 & b_1 & b_0 & \\ 0 & 0 & b_2 & b_1 & b_0 & \\ a_3^{(2)} & 0 & b_2 & b_1 & b_0 & \\ a_4^{(2)} & a_3^{(2)} & & b_2 & b_1 & b_0 \\ a_5^{(2)} & a_4^{(2)} & & b_2 & b_1 \\ & a_5^{(2)} & & & b_2 & b_1 \end{bmatrix}$$

- the corresponding polynomial operation has the form

•

$$h_2(x) := a_3^{(2)} x^2 + a_4^{(2)} x + a_5^{(2)} = h_3(x) - g(x)(a_2^{(1)}/b_0)x.$$

This process can be continued : the coefficient $a_3^{(2)}$ is reduced to zero. We have

$$S^{(3)}(f,g) = S^{(2)}(f,g)E_{6,1}(rac{a_3^{(2)}}{b_0})E_{7,2}(rac{a_3^{(2)}}{b_0})$$

 $h_1(x):=a_4^{(3)}x+a_5^{(3)}=h_2(x)-g(x)(a_2^{(3)}/b_0)$ The matrix $S^{(3)}(f,g)$ has the form

$$S^{(3)}(f,g) = egin{bmatrix} 0 & b_0 & & \ 0 & 0 & b_1 & b_0 & \ 0 & 0 & b_2 & b_1 & b_0 & \ 0 & 0 & b_2 & b_1 & b_0 & \ a^{(3)}_4 & 0 & & b_2 & b_1 & b_0 & \ a^{(3)}_5 & a^{(3)}_4 & & & b_2 & b_1 & \ a^{(3)}_5 & a^{(3)}_4 & & & b_2 & b_1 & \ a^{(3)}_5 & a^{(3)}_5 & & & b_2 & \end{bmatrix}$$

۰

We finaly have

$$\underbrace{\underbrace{a_0x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5}_{f_0(x) = f(x)} = \\ \underbrace{\left((a_0/b_0)x^3 + (a_2^{(1)}/b_0)x + (a_3^{(2)}/b_0)\right)}_{q_0(x)} \underbrace{\left(b_0x^2 + b_1x + b_2\right)}_{f_1(x) = g(x)} \\ + \underbrace{\left(a_4^{(3)}x + a_5^{(3)}\right)}_{f_2(x)}.$$

Now we summarize all previous transformations. Let us put

$$T_{1} = E_{3,1}(\frac{a_{0}}{b_{0}})E_{4,2}(\frac{a_{0}}{b_{0}})E_{4,1}(\frac{a_{1}^{(1)}}{b_{0}})E_{5,2}(\frac{a_{1}^{(1)}}{b_{0}})E_{5,1}(\frac{a_{2}^{(2)}}{b_{0}})E_{6,2}(\frac{a_{2}^{(2)}}{b_{0}})E_{6,1}(\frac{a_{3}^{(3)}}{b_{0}})E_{7,2}(\frac{a_{3}^{(3)}}{b_{0}})P$$

where $P \in \mathbb{R}^{7 \times 7}$ is the permutation matrix

$$P = (e_3, e_4, e_5, e_6, e_7, e_1, e_2).$$

It is easy to see that

$$S^{(4)}(f,g) := S(f,g)T_1 = egin{bmatrix} b_0 & & & & \ b_2 & b_1 & b_0 & & \ & b_2 & b_1 & b_0 & & \ & & b_2 & b_1 & | & b_0 & a_4^{(4)} & \ & & b_2 & | & b_1 & a_5^{(4)} & a_4^{(4)} \ & & & | & b_2 & & a_5^{(4)} \end{bmatrix}$$

and the transformation T_1 corresponds the above polynomial operation which is equivalent to one step of the recursion corresponding to i = 0.

 $f_i(x) = q_i(x)f_{i+1}(x) + f_{i+2}(x), \quad i = 0, 1, 2, \dots$

Moreover, the marked 3×3 submatrix is a Sylvester matrix $S(f_1, f_2)$.

The transformation of $S(f_1, f_2)$ to triangular form is carried out in the same way as above, if $f_2 \neq 0$. In the opposite case $f_1 = \text{GCD}(f_0, f_1)$. Let us mention once more the Euclide's algorithm.

 $f_i(x) = q_i(x)f_{i+1}(x) + f_{i+2}(x), \quad i = 0, 1, 2, \dots$

ullet deg $f_{i+2} <$ deg $f_{i+1}.$

In general case there exist T_1 and s such that if we denote $n_2 = m - i_s$, $f_2(x) = a_{i_s}^{(s)} x^{n_2} + a_{i_s+1}^{(s)} x^{n_2-1} + \dots + a_m^{(s)}$

then the matrix $S^{(s+1)}(f,g)=S(f,g)T_1$ has the form



In this case the inequality

(4) $\operatorname{rank}(S(f_0, f_1)) = m - \deg(f_2) + \operatorname{rank}(S(f_1, f_2))$

holds.

If $f_2 = 0$ then f_1 divides f_0 and $rank(S(f_0, f_1)) = m$. If we transform $S(f_1, f_2)$, afterwards $S(f_2, f_3)$, ... then the repetition of (4) leads to the following result:

Theorem 2.1 Let f and g be the polynomials of degrees m and n respectively. Then the following statements are equivalent:

1. rank $(S(f,g)) = m + n - k \Leftrightarrow \deg(\mathsf{GCD}(f,g)) = k;$

2. rank $(S(f,g)) < m + n - k \Leftrightarrow \deg(\operatorname{GCD}(f,g)) > k;$

The analogous considerations with S_k yields the following theorem.

Theorem 2.2 Let f and g be the polynomials of degrees m and n respectively, $1 \le k \le \min(m, n)$ and let S_k be the kth Sylvester submatrix. Then the following statements are equivalent: 1. rank $(S_k) = m + n - 2k + 1 \Leftrightarrow \deg(\mathsf{GCD}(f,g)) = k;$

2. rank $(S_k) \leq m+n-2k+1 \Leftrightarrow {\sf deg}\;({\sf GCD}(f,g)) \geq k.$

3. A low rank approximation of the Sylvester matrix

A low rank approximation of the Sylvester matrix This section considers the use of the method of

structured total least norm (STLN)

(Ben Rosen, Kaltofen, Yang, Zhi, Winkler) for the construction of a structured low rank approximation of the Sylvester matrix for approximate GCD computations. Let an integer k, $1 \le k \le \min(m, n)$ be given. Required: Perturbations $\delta f(x)$ and $\delta g(x)$ of f(x) and g(x) respectively,

$$egin{array}{lll} \delta f(x) &=& \delta a_0 x^m + \delta a_1 x^{m-1} + \cdots + \delta a_{m-1} x + \delta a_m, \ \delta g(x) &=& \delta b_0 x^n + \delta b_1 x^{n-1} + \cdots + \delta b_{n-1} x + \delta b_n, \end{array}$$

deg $(\operatorname{GCD}(f+\delta f,g+\delta g)) \geq k$ and $\|\delta f\|_2^2 + \|\delta g\|_2^2$ is minimised.

The kth Sylvester submatrix has the form

$$S_{k} = \begin{bmatrix} c_{k} & A_{k} \\ a_{0} & b_{0} & b_{1} & b_{0} \\ a_{1} & a_{0} & b_{1} & b_{0} \\ \vdots & a_{1} & \vdots & b_{1} & \vdots \\ \vdots & \vdots & a_{0} & \vdots & b_{0} \\ a_{m} & \vdots & a_{1} & b_{n} & \vdots & b_{1} \\ a_{m} & \vdots & \vdots & \vdots & \vdots \\ a_{m} & \vdots & \vdots & \vdots & \vdots \\ \vdots & a_{m} & b_{n} \end{bmatrix} \cdot (m + n - (k - 1))$$

$$S_{k} = [c_{k}, A_{k}] ,$$

 $c_k \in \mathbb{R}^{m+n-k+1}$ and $A_k \in \mathbb{R}^{(m+n-k+1) imes (m+n-2k+1)}$. According to this notation we can formulate the following lemma.

Lemma 3.1 Let f and g be polynomials of degrees mand n respectively, $1 \le k \le \min(m, n)$ and let S_k be the kth Sylvester submatrix. Then the following statements are equivalent:

a) $\deg(\operatorname{GCD}(f_0,f_1))=k\Leftrightarrow \operatorname{rank}(A_k)=m+n-2k+1$ and the dimension of the null space of S_k is equal to one. b) $\deg(\operatorname{GCD}(f_0, f_1)) > k \Leftrightarrow \operatorname{rank}(A_k) < m + n - 2k + 1$ and the dimension of the null space of S_k is at least two.

(Kaltofen, Yang, Zhi, Wikler).

Theorem 4.1 Let f and g be the polynomials of degrees m and n respectively, $1 \le k \le \min(m, n)$ and S_k the kth Sylvester submatrix. Let $S_k = [c_k, A_k]$ where c_k is the first column of the matrix S_k . Then the following statements are equivalent:

a) $\deg(\operatorname{GCD}(f,g)) = k \Leftrightarrow$ the equation $A_k y = c_k$ possesses exactly one nontrivial solution.

b) $\deg(\operatorname{GCD}(f,g)) > k \Leftrightarrow$ the equation $A_k y = c_k$ possesses at least two linearly independent solutions.

Now we describe the STLN method The polynomials f(x) and g(x) can be inexact. For a given integer $k \in [1, \min(m, n)]$ we want to compute the minimal perturbation of the coefficients of f(x) and g(x) such that

the degree of greatest common divisors of the perturbed polynomials equals k.

...to compute a perturbation matrix $[h_k,\,E_k]$ with the same block structure as $[c_k,\,A_k]$ such that the equation

 $(A_k + E_k)y = c_k + h_k$ $y = [y_1, y_2, \dots, y_{m+n-2k+1}]^T$

possesses exactly one nontrivial solution. Hence we solve the constrained minimisation problem,

 $\min \left\| \left[\begin{array}{cc} h_k & E_k \end{array}
ight]
ight\|_F$ such that $(A_k + E_k)y = c_k + h_k.$

 $\ldots z_i$ is the perturbation of a_i for $i=0,\ldots,m,$

 $\ldots z_{m+i+1}$ is the perturbation of b_i for $i=0,\ldots,n$.

The structured error matrix $[h_k, E_k] \in \mathbb{R}^{(m+n-k+1) imes (m+n-2k+2)}$

 $egin{bmatrix} z_0 & | & z_0 & | & z_{m+1} \ z_1 & | & z_1 & \ddots & | & z_{m+2} & z_{m+1} \ dots & do$

Define the (m+n-k+1) imes (m+n+2) matrix $Y_k=$

٠

and the matrix $P_k \in \mathbb{R}^{(m+n-k+1) imes (m+n+2)},$

$$P_k = \left[egin{array}{cc} I_{m+1} & 0 \ 0 & 0 \end{array}
ight].$$

 $h_k = P_k z$, and $Y_k(y)z = E_k(z)y$.

The residual vector

$$r = r(z, y) = c_k + h_k - (A_k + E_k)y.$$

The STLN method.

We seek a vector $\boldsymbol{z} = [z_0, z_1, \dots, z_{m+n+1}]^T \in \mathbb{R}^{m+n+2}$ such that the system

 $(A_k + E_k(z))y = c_k + h_k(z)$

has just one nontrivial solution and

 $||z||_2$ is minimal.

 $(\|Dz\|_2)$ is minimal.

Let z and y be initial approximations.

We express $r(z+\delta z,y+\delta y)$ as the lowest order Taylor series and we try to calculate shifts $\delta z,\delta y$ such that

$$\approx r(z,y) \underbrace{\frac{r(z+\delta z,y+\delta y)\approx 0}{-(Y_k-P_k)\delta z-(A_k+E_k)\delta y}}_{$$

This leads to the iterative process for δy and δz where in

the each stage the LSE problem is solved (See Winkler):

$$egin{aligned} &\min_{\delta z} & \left[egin{aligned} D & 0 \end{array}
ight] \left[egin{aligned} \delta z \ \delta y \end{array}
ight] - (-Dz)
ight] & ext{subject to} \ & \| (D(z+\delta z) \| \ & \|$$

where

 $D = diag(D_1, D_2), \quad D_1 = (n-k+1)I_{m+1}, \quad D_2 = (m-k+1)I_{n+1}.$

Denoting

$$egin{aligned} C &= ig[\left(Y_k - P_k
ight) \; \left(A_k + E_k
ight) ig] \in \mathbb{R}^{(m+n-k+1) imes (2m+2n-2k+3)} \ E &= ig[D \; 0 \; ig] \in \mathbb{R}^{(m+n+2) imes (2m+2n-2k+3)} \ q &= r(z,y) \in \mathbb{R}^{m+n-k+1} \ p &= -Dz \in \mathbb{R}^{m+n+2} \ w &= igg[rac{\delta z}{\delta y} igg] \in \mathbb{R}^{2m+2n-2k+3}, \end{aligned}$$

We can see that the computation of an approximate GCD reduces to the LSE problem

$$\min_{w} \| Ew - p \|_2$$
 subject to $Cw = q,$

where the dimensions of the matrices and vectors are: $C\in \mathbb{R}^{m_1 imes t}$, $E\in \mathbb{R}^{m_2 imes t}$, $w\in \mathbb{R}^t$, $q\in \mathbb{R}^{m_1}$, $p\in \mathbb{R}^{m_2}$ where

 $m_1 = m + n - k + 1$, $m_2 = m + n + 2$ and t = 2m + 2n - 2k + 3.

Consider the exact polynomials

$$\hat{f}(x) = (x - 0.25)^8 (x - 0.5)^9 (x - 0.75)^{10} (x - 1)^{11} (x - 1.25)^{12}$$

and

$$\hat{g} = (x + 0.25)^4 (x - 0.25)^5 (x - 0.5)^6$$

which have 11 common roots and hence $\operatorname{rank}(S(\widehat{f},g) = 54$. The coefficients of these polynomials were perturbed by noise corresponding to the different values of μ (the signal-to-noise ratio). The given inexact polynomials fand g are constructed by perturbing \widehat{f} and \widehat{g} respectively. Let c_f and c_g be vectors $\in \mathbb{R}^{n+1}$ of random variables uniformly distributed in the interval [-1, ..., +1]. Let $\varepsilon = 1/\mu$, the inexact polynomials



The legitimate solution fulfill the inequalities

(1)
$$||z_f|| \le \frac{||f||}{\mu} \qquad \frac{||z_g||}{\alpha} \le \frac{||g||}{\mu},$$

where $z_g \in \mathbb{R}^{n+1}$ stores the structured perturbation of the polynomial αg . For each value α the values $||z_f||$, $||z_g||$ and $r_{norm} = r(z, y)/||c_k + h_k||$ are stored.

The values of α for the values ||f|| and ||g|| that satisfy
 (1) and

$$|r_{norm}\| \le 10^{-12}$$

are retained.

• For each acceptable value α compute singular values σ_i of $S(\hat{f}, \hat{g})$, where \hat{f} and \hat{g} are computed and normalized polynomials.

• The singular values are arranged in non-increasing order and the value α is found for which the ratio $\sigma_{m+n-k}/\sigma_{m+n-k+1}$ attains a maximum. The polynomials that corresponds to this value of α are the solution.

The following graphs are for $\mu = 10^8$. The *y*-axis in the following plots are logarithmic.



(a) The maximum allowable value of $\|z_f\|$ which is equal to $\|f\|/\mu$, (b) The computed value of $\|z_f\|$;



(a)The maximum allowable value of $||z_g||/\alpha$ which is equal to $||g||/\mu$, (b) The computed value of $||z_g||/\alpha$;



The normalized residual norm $||r_{norm}||$;



the singular value ratio σ_{54}/σ_{55}



The normalized singular values of the Sylvester matrix for \diamond ... the theoretically exact data $S(\hat{f}, \hat{g})$; \Box ... the given inexact data S(f, g);

 \times ... the computed data $S(f_0, g_0)$;



the same for $\alpha = 10^{1.4}$;

The End Thank you for your attention!