Analysis and numerical experiments connected with the computing of an AGCD of two inexact polynomials

Jan Zítko, Jan Kuřátko

Charles University, Faculty of Mathematics and Physics,
Department of Numerical Mathematics, Prague

PANM 15, Dolní Maxov, June 6 – 11, 2010

Overview:

1: Notation

2: Euclid's algorithm and transformations of Sylvester matrix

3: Inexact polynomials

4: Computing the GCD using c-s transformation

5: QR-factorization method for computing the greatest common divisor

1. Notation

Two well-known methods for computing the GCD:

- the Euclid's algorithm
- manipulations with the Sylvester matrix

Let

deg(f)...the degree of f;

GCD (f, g) ...the greatest common divisor of f a g.

$$f(x) = a_0x^m + a_1x^{m-1} + \cdots + a_{m-1}x + a_m,$$
$$g(x) = b_0x^n + b_1x^{n-1} + \cdots + b_{n-1}x + b_n,$$

where $m \geq n$, $a_0\, a_m \neq 0$, $b_0\, b_n \neq 0$.

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

$$S(f,g) = \begin{bmatrix} a_0 & a_1 & \ldots & a_{m-1} & a_m & 0 & \ldots & 0 \\ 0 & a_0 & \ldots & \ldots & a_{m-1} & a_m & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & a_0 & a_1 & \ldots & a_{m-1} & a_m \\ - & - & - & - & - & - & - & - \\ b_0 & b_1 & \ldots & b_{n-1} & b_n & 0 & \ldots & 0 \\ 0 & b_0 & \ldots & \ldots & b_{n-1} & b_n & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & b_0 & b_1 & \ldots & b_{n-1} & b_n \end{bmatrix}.$$

The kth Sylvester subresultant $S_k \in \mathbb{C}^{(m+n-2k+2)\times(m+n-k+1)}$ is formed from $S(f,g)$ by deleting the last $(k-1)$ columns, the last $(k-1)$ row of the coefficients of f and the last $(k-1)$ row of the coefficients of g.

2. Euclid's algorithm and transformations of Sylvester matrix

Let us define $f_0 := f$ and $f_1 := g$. The polynomials in the successive divisions in Euclid's algorithm are defined by

$$f_j(x) = f_{j+1}(x)q_j(x) + f_{j+2}(x), \quad j = 0, 1, 2, \ldots \ ,$$

where $\deg f_{j+2} < \deg f_{j+1}$.
If $f_{t+1} = 0$ and $f_j \neq 0 \ \forall j \leq t$ then $f_t = \mathrm{GCD}(f_0, f_1)$.

For illustration, let f_0 and f_1 be of degrees 5 and 2 respectively:

$$f_0(x) = a_0x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5,$$
$$f_1(x) = b_0x^2 + b_1x + b_2.$$

The Sylvester matrix $S(f_0, f_1)$ for the polynomials f_0 and f_1 is

$$S(f_0, f_1) = \begin{bmatrix} a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & 0 \\ 0 & a_0 & a_1 & a_2 & a_3 & a_4 & a_5 \\ b_0 & b_1 & b_2 & 0 & 0 & 0 & 0 \\ 0 & b_0 & b_1 & b_2 & 0 & 0 & 0 \\ 0 & 0 & b_0 & b_1 & b_2 & 0 & 0 \\ 0 & 0 & 0 & b_0 & b_1 & b_2 & 0 \\ 0 & 0 & 0 & 0 & b_0 & b_1 & b_2 \end{bmatrix}.$$

Now we will formulate the modified Euclid's algorithm:

$$c_0 \underbrace{(a_0x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5)}_{f_0(x)} + s_0 \underbrace{(b_0x^2 + b_1x + b_2)}_{f_1(x)} x^3$$

$$\underbrace{= 0 + \underbrace{(c_0a_1 + s_0b_1)}_{a_1^{(1)}} x^4 + \underbrace{(c_0a_2 + s_0b_2)}_{a_2^{(1)}} x^3 + \underbrace{c_0a_3}_{a_3^{(1)}} x^2 + \underbrace{c_0a_4}_{a_4^{(1)}} x + \underbrace{c_0a_5}_{a_5^{(1)}}}_{h_4(x) := a_1^{(1)}x^4 + a_2^{(1)}x^3 + a_3^{(1)}x^2 + a_4^{(1)}x + a_5^{(1)}}.$$

$$G_0^{(1)}(c_0, s_0) := \begin{bmatrix} c_0 & 0 & s_0 & 0 & 0 & 0 & 0 \\ 0 & c_0 & 0 & s_0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

$$S^{(1)}(f_0, f_1) := G_0^{(1)}(c_0, s_0) S(f_0, f_1)$$

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

where

$$a_i^{(1)} = \begin{cases} c_0 a_i + s_0 b_i & \text{for} \quad i = 1, 2 \\ c_0 a_i & \text{otherwise} \end{cases}.$$

Let $a_1^{(1)} \neq 0$. Then deg$(h_4) = 4$. In the opposite case, the process would be performed with the polynomial of degree less than 4. The Euclid's algorithm proceeds according to the following schema:

$$c_1 \underbrace{\left(a_1^{(1)} x^4 + a_2^{(1)} x^3 + a_3^{(1)} x^2 + a_4^{(1)} x + a_5^{(1)}\right)}_{h_4(x)} + s_1 \underbrace{\left(b_0 x^2 + b_1 x + b_2\right)}_{f_1(x)} x^2$$
$$\underbrace{= 0 + \underbrace{\left(c_1 a_2^{(1)} + s_1 b_1\right)}_{a_2^{(2)}} x^3 + \underbrace{\left(c_1 a_3^{(1)} + s_1 b_2\right)}_{a_3^{(2)}} x^2 + \underbrace{c_1 a_4^{(1)}}_{a_4^{(2)}} x + \underbrace{c_1 a_5^{(1)}}_{a_5^{(2)}}}_{h_3(x) := a_2^{(2)} x^3 + a_3^{(2)} x^2 + a_4^{(2)} x + a_5^{(2)}}$$

The numbers c_1 a s_1 are again chosen to remove the coefficient by x^4. The corresponding matrix operation consists of premultiplying

$G_1^{(1)}(c_1, s_1)S^{(1)}(f_0, f_1)$, where

$$G_1^{(1)}(c_1, s_1) = \begin{bmatrix} c_1 & 0 & 0 & s_1 & 0 & 0 & 0 \\ 0 & c_1 & 0 & 0 & s_1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

We obtain $S^{(2)}(f_0, f_1) := G_1^{(1)}(c_1, s_1)S^{(1)}(f_0, f_1)$

$$= \begin{bmatrix} 0 & 0 & a_2^{(2)} & a_3^{(2)} & a_4^{(2)} & a_5^{(2)} & 0 \\ 0 & 0 & 0 & a_2^{(2)} & a_3^{(2)} & a_4^{(2)} & a_5^{(2)} \\ b_0 & b_1 & b_2 & 0 & 0 & 0 & 0 \\ 0 & b_0 & b_1 & b_2 & 0 & 0 & 0 \\ 0 & 0 & b_0 & b_1 & b_2 & 0 & 0 \\ 0 & 0 & 0 & b_0 & b_1 & b_2 & 0 \\ 0 & 0 & 0 & 0 & b_0 & b_1 & b_2 \end{bmatrix},$$

where

$$a_i^2 = \begin{cases} c_1 a_i^{(1)} + s_1 b_{i-1} & \text{for} \quad i = 2, 3 \\ c_1 a_i^{(1)} & \text{otherwise} \end{cases} .$$

Let $a_2^2 \neq 0$. Let the numbers c_2, s_2 and then c_3 a s_3 remove the coefficients by dominant power. The last two divisions yield the polynomials

$$\begin{aligned} h_2(x) &= a_3^{(3)} x^2 + a_4^{(3)} x + a_5^{(3)} &&= c_2 h_3(x) + s_2 f_1(x) x \\ h_1(x) &= a_4^{(4)} x + a_5^{(4)} &&= c_3 h_2(x) + s_3 f_1(x) \end{aligned} ,$$

where $a_3^{(3)} \neq 0$ and $a_4^{(4)} \neq 0$.

If we analogously define the matrices $G_2^{(1)}(c_2, s_2)$, $G_3^{(1)}(c_3, s_3)$, then
$S^{(4)}(f_0, f_1) := G_3^{(1)}(c_3, s_3)G_2^{(1)}(c_2, s_2)S^{(2)}(f_0, f_1)$

$$= \begin{bmatrix} 0 & 0 & 0 & 0 & a_4^{(4)} & a_5^{(4)} & 0 \\ 0 & 0 & 0 & 0 & 0 & a_4^{(4)} & a_5^{(4)} \\ b_0 & b_1 & b_2 & 0 & 0 & 0 & 0 \\ 0 & b_0 & b_1 & b_2 & 0 & 0 & 0 \\ 0 & 0 & b_0 & b_1 & b_2 & 0 & 0 \\ 0 & 0 & 0 & b_0 & b_1 & b_2 & 0 \\ 0 & 0 & 0 & 0 & b_0 & b_1 & b_2 \end{bmatrix}.$$

Define

$$G_1 = G_3^{(1)}(c_3, s_3)G_2^{(1)}(c_2, s_2)G_1^{(1)}(c_1, s_1)G_0^{(1)}(c_0, s_0)$$

and

$$P_1 = [e_3, e_4, e_5, e_6, e_7, e_1.e_2] \ .$$

Then the first stage of Euclid' algorithm can be written in matrix formulation as follows

$$P_1G_1S(f_0,f_1)=\left[\begin{array}{cccc|ccc} b_0 & b_1 & b_2 & 0 & 0 & 0 & 0\\ 0 & b_0 & b_1 & b_2 & 0 & 0 & 0\\ 0 & 0 & b_0 & b_1 & b_2 & 0 & 0\\ 0 & 0 & 0 & b_0 & b_1 & b_2 & 0\\ \hline 0 & 0 & 0 & 0 & b_0 & b_1 & b_2\\ 0 & 0 & 0 & 0 & a_4^{(4)} & a_5^{(4)} & 0\\ 0 & 0 & 0 & 0 & 0 & a_4^{(4)} & a_5^{(4)} \end{array}\right].$$

We have obtained the coefficients of the polynomial h_1 in the last two rows. Summarizing all steps of the first stage of Euclidean algorithm, we obtain

$$\underbrace{c_3c_2c_1c_0f_0(x)}_{\widetilde{f_0}(x)}=\underbrace{-(c_3c_2c_1s_0x^3+c_3c_2s_1x^2+c_3s_2x+s_3)}_{\widetilde{q_0}(x)}\underbrace{f_1(x)}_{\widetilde{f_1}(x)}+\underbrace{h_1(x)}_{\widetilde{f_2}(x)}.$$

Hence we have

$$\widetilde{f_0}(x)=\widetilde{q_0}(x)\widetilde{f_1}(x)+\widetilde{f_2}(x).$$

We will shortly demonstrate on our illustrative example how to pick the numbers c and s. If we take

$$c_0 = 1 \qquad \text{and} \qquad s_0 = -\frac{a_0}{b_0} \; .$$

then the division in Euclid's algorithm has the following form

$$\underbrace{(a_0x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5)}_{f_0(x)} - \underbrace{(b_0x^2 + b_1x + b_2)}_{f_1(x)}\left(\frac{a_0}{b_0}\right)x^3$$

$$= 0 + \underbrace{\left(a_1 - \frac{a_0b_1}{b_0}\right)}_{a_1^{(1)}} x^4 + \underbrace{\left(a_2 - \frac{a_0b_2}{b_0}\right)}_{a_2^{(1)}} x^3 + \underbrace{a_3}_{a_3^{(1)}} x^2 + \underbrace{a_4}_{a_4^{(1)}} x + \underbrace{a_5}_{a_5^{(1)}}$$

The second choice of c and s in the first step:

$$c_0 = \frac{b_0}{\sqrt{a_0^2 + b_0^2}} \qquad \text{a} \qquad s_0 = -\frac{a_0}{\sqrt{a_0^2 + b_0^2}} \; .$$

We will again use the original notation, f and g for polynomials, m =deg(f) and n =deg(g).

Theorem 3.1 *Let f and g be the polynomials of degrees m and n respectively. It is assumed that the polynomials $f_0(x), f_1(x), f_2(x), \ldots,$ which are constructed by Euclid's algorithm satisfy: $f_{t+1} = 0$, $f_j \neq 0$ for $j \leq t$. The following statements hold:*

1) *There exists a nonsingular matrix Z of order $m+n$ such that the matrix $ZS(f,g)$ has the block form*

$$ZS(f,g) = \left[\begin{array}{c|c} R_U & R_{1,2} \\ \hline 0 & R_{2,2} \end{array}\right],$$

where $\boldsymbol{R_U}$ *is a square upper triangular matrix with non-zero diagonal elements, and* $\boldsymbol{R_{2,2}}$*, the resultant matrix after transformation of the Sylvester resultant matrix* $\boldsymbol{S(f_{t-1}, f_t)}$*, is a square upper triangular matrix of order* $(\boldsymbol{n_{t-1}}+\boldsymbol{n_t})$*. The matrix* $\boldsymbol{R_{2,2}}$ *has the following forms:*

(a) If $\boldsymbol{n_t > 0}$*, then the first* $\boldsymbol{n_{t-1}}$ *diagonal elements of* $\boldsymbol{R_{2,2}}$ *are non-zero. The last* $\boldsymbol{n_k}$ *rows of* $\boldsymbol{R_{2,2}}$ *are zero.*

The polynomial $\boldsymbol{f_t}$ *is equal to the GCD of* $(\boldsymbol{f}, \boldsymbol{g})$*.*

(b) If $n_t = 0$, then $f_t =: c \neq 0$ and $R_{2,2} = cI_{n_{t-1}}$. In this case rank $S(f,g) = m + n$.

Theorem 3.2 *Let f and g be the polynomials* of degrees m and n respectively, $1 \leq k \leq \min(m,n)$ and let S_k be the kth Sylvester subresultant. Then the following statements are equivalent:

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

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

$$\text{rank } S_k = m+n-2k+1 \Leftrightarrow \text{deg GCD}(f,g) = k,$$

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

3. Inexact polynomials

The kth Sylvester subresultant has the form

$$
S_k \quad = \quad \left.\begin{array}{l}
\underbrace{\left[\begin{array}{cccccccc}
a_0 & a_1 & \dots & a_{m-1} & a_m & 0 & \dots & 0 \\
\hline
0 & a_0 & \dots & a_{m-2} & a_{m-1} & a_m & \dots & 0 \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
0 & \dots & 0 & a_0 & a_1 & \dots & a_{m-1} & a_m \\
\hline
b_0 & b_1 & \dots & b_{n-1} & b_n & 0 & \dots & 0 \\
0 & b_0 & \dots & & b_{n-1} & b_n & \dots & 0 \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
0 & \dots & 0 & b_0 & b_1 & \dots & b_{n-1} & b_n
\end{array}\right]}_{m+n-(k-1)}
\end{array}
\begin{array}{l}
u_k^T \text{ (the first row)} \\
\\
\\
n-(k-1) \\
\\
\\
m+n-2k+2 \\
\\
\end{array}\right\} = \left[\begin{array}{c} u_k^T \\ \\ A_k^T \\ \\ \\ \end{array}\right]
$$

$$
S_k = \left[\begin{array}{c} u_k^T \\ A_k^T \end{array}\right], \text{ where}
$$

$u_k \in \mathbb{R}^{m+n-k+1}$ and $A_k \in \mathbb{R}^{(m+n-2k+1)\times(m+n-k+1)}$.

Theorem 3.3 *Let f and g be the polynomials of degrees m and n respectively, $1 \leq k \leq \min(m,n)$ and S_k the kth Sylvester subresultant. Let $S_k^T = [u_k, A_k]$ where u_k is the first column of the matrix S_k^T Then the following statements are equivalent:*

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

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

(Ben Rosen, Kaltofen, Yang, Zhi, Winkler)

Let an integer k, $1 \leq k \leq \min(m, n)$ be given.
We seek perturbations $\delta f(x)$ and $\delta g(x)$ of $f(x)$ and $g(x)$ respectively,

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

such that

$$\begin{aligned} &\deg\,(\mathrm{GCD}(f + \delta f, g + \delta g)) \geq k \quad \text{and} \\ &\|\delta f\|^2 + \|\delta g\|^2 \text{ is minimal.} \end{aligned}$$

The polynomials $f(x)$ and $g(x)$ are inexact, an 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 the greatest common divisors of perturbed polynomials equals k.

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

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

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

$$\min \left\| \left[\, h_k \;\; E_k \, \right] \right\|_F \quad \text{such that} \quad (A_k + E_k) y = u_k + h_k.$$

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

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

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

$$
\begin{array}{c}
\left[\begin{array}{c|ccc|ccccc}
z_0 & & & & z_{m+1} & & & & \\
z_1 & z_0 & \ddots & & \vdots & z_{m+2} & \ddots & & \\
\vdots & \vdots & \ddots & z_0 & z_{m+n} & \vdots & \ddots & z_{m+1} & \\
z_{m-1} & \vdots & \ddots & z_1 & z_{m+n+1} & z_{m+n} & & z_{m+2} & z_{m+1} \\
z_m & z_{m-1} & \ddots & \vdots & & z_{m+n+1} & \ddots & \vdots & z_{m+2} \\
 & z_m & \ddots & \vdots & & & \ddots & z_{m+n} & \vdots \\
 & & & z_{m-1} & & & & z_{m+n+1} & z_{m+n} \\
 & & & z_m & & & & & z_{m+n+1}
\end{array}\right]. \\
\begin{array}{ccc}
\underbrace{\qquad\quad}_{h_k} & \underbrace{\qquad\qquad\qquad\qquad}_{n-k} & \underbrace{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}_{m-k+1}
\end{array}
\end{array}
$$

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

$$\left[\underbrace{\begin{array}{ccccc} 0 & & & & \\ y_1 & & & & \\ \cdot & y_1 & & & \\ \cdot & \cdot & \cdot & & \\ y_{n-k} & \cdot & \ddots & y_1 & \\ & y_{n-k} & \ddots & \cdot & y_1 \\ & & \ddots & \cdot & \cdot \\ & & \ddots & y_{n-k} & \cdot \\ & & & & y_{n-k} \\ & & & & \end{array}}_{m+1} \middle| \underbrace{\begin{array}{ccccc} y_{n-k+1} & & & & \\ y_{n-k+2} & y_{n-k+1} & & & \\ \cdot & y_{n-k+2} & \ddots & & \\ \cdot & \cdot & \ddots & \ddots & \\ \cdot & \cdot & \ddots & \ddots & y_{n-k+1} \\ y_{m+n-2k+1} & \cdot & \ddots & \ddots & y_{n-k+2} \\ & y_{m+n-2k+1} & \ddots & \ddots & \cdot \\ & & \ddots & \ddots & \cdot \\ & & & \ddots & \cdot \\ & & & & y_{m+n-2k+1} \end{array}}_{n+1} \right].$$

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

$$P_k = \begin{bmatrix} I_{m+1} & 0 \\ 0 & 0 \end{bmatrix}.$$

$$h_k = P_k z, \quad \text{and} \quad Y_k(y)z = E_k(z)y \;\; !!!$$

The residual vector

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

The SNTL method.

We seek a vector $z = \{z_0, z_1, \ldots, z_{m+n+1}\} \in \mathbb{R}^{m+n+1}$

such that the system

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

has just one nontrivial solution and

$\|z\|_2$ is minimal.

Let z and y be initial aproximations.
We express $r(z+\delta z, y+\delta y)$ and we try to calculate shifts $\delta z, \delta y$ such that

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

This leads to the iterative process for δy and δz where in the each stage the LSE problem is solved (See Reference Winkler, Kaltofen):

$$\min_{\delta z} \underbrace{\left\| \begin{bmatrix} D & 0 \end{bmatrix} \begin{bmatrix} \delta z \\ \delta y \end{bmatrix} - (-Dz) \right\|}_{\|(D(z+\delta z)\|} \quad \text{subject to}$$

$$\underbrace{\begin{bmatrix} (Y_k - P_k) & (A_k + E_k) \end{bmatrix} \begin{bmatrix} \delta z \\ \delta y \end{bmatrix} = r(z,y).}_{r(z+\delta z, y+\delta y)=0}$$

where

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

Denoting

$$
\begin{aligned}
\boldsymbol{B} &= \left[\ (\boldsymbol{Y_k} - \boldsymbol{P_k}) \quad , \quad (\boldsymbol{A_k} + \boldsymbol{E_k})\ \right] \in \mathbb{R}^{(m+n-k+1)\times(2m+2n-2k+3)} \\
\boldsymbol{A} &= \left[\ \boldsymbol{D} \quad \boldsymbol{0}\ \right] \in \mathbb{R}^{(m+n+2)\times(2m+2n-2k+3)} \\
\boldsymbol{d} &= \boldsymbol{r(z,y)} \in \mathbb{R}^{m+n-k+1} \\
\boldsymbol{b} &= -\boldsymbol{Dz} \in \mathbb{R}^{m+n+2} \\
\boldsymbol{w} &= \left[\begin{array}{c} \boldsymbol{\delta z} \\ \boldsymbol{\delta y} \end{array}\right] \in \mathbb{R}^{2m+2n-2k+3},
\end{aligned}
$$

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

$$
\min_{\boldsymbol{w}} \|\boldsymbol{Aw} - \boldsymbol{b}\|_2 \quad \text{subject to} \quad \boldsymbol{Bw} = \boldsymbol{d}. \tag{1}
$$

[Björk, Van Loan]

The exact polynomials $\hat{f}$ and $\hat{g}$:

$$\hat{f}(x) = \hat{a}_0 x^m + \hat{a}_1 x^{m-1} + \cdots + \hat{a}_{m-1} x + \hat{a}_m,$$
$$\hat{g}(x) = \hat{b}_0 x^n + \hat{b}_1 x^{n-1} + \cdots + \hat{b}_{n-1} x + \hat{b}_n.$$

$\|\hat{f}(x)\|$ denotes the Euclidean norm

$c_f \in \mathbb{R}^{m+1}$ and $c_g \in \mathbb{R}^{n+1}$ ...random vectors with components in $[-1,\ 1]$ and ϵ a small positive number (perturbation)

$$\delta \hat{a}_i = \epsilon \frac{\|\hat{f}\|}{\|c_f\|} c_{f,\,i}\,,$$

$c_{f,\,i}$ ... th ith component of c_f, $i = 0, 1, \ldots, m$. The perturbation of g is defined analogously. Let us write

$$f = \hat{f} + \epsilon \frac{\|\hat{f}\|}{\|c_f\|} c_f; \quad f(x) = \sum_{i=0}^{m} (\hat{a}_i + \delta \hat{a}_i) x^{m-i} =: \sum_{i=0}^{m} a_i x^{m-i}$$
$$g = \hat{g} + \epsilon \frac{\|\hat{g}\|}{\|c_g\|} c_g; \quad g(x) = \sum_{i=0}^{n} (\hat{b}_i + \delta \hat{b}_i) x^{n-i} =: \sum_{i=0}^{n} a_i x^{n-i}$$

Polynomials $f(x)$ and $g(x)$ are rearranged:

$$f(x) = \sum_{i=0}^{m} \tilde{a}_i x^{m-i}, \qquad \tilde{a}_i = \frac{a_i}{\left(\prod_{k=0}^{m} |a_k|\right)^{\frac{1}{m+1}}},$$

$$g(x) = \sum_{i=0}^{n} \tilde{b}_i x^{n-i}, \qquad \tilde{b}_i = \frac{b_i}{\left(\prod_{k=0}^{n} |b_k|\right)^{\frac{1}{n+1}}},$$

Example 1. (Ján Eliaš) $\mu = 10^6$. Exact polynomials

$$\hat{f}(x) = (x-1.2)^4(x+2)^5(x-0.5)^4,$$
$$\hat{g}(x) = (x-1.4)^2(x+2)^3(x-0.5)^4.$$

It is immediately to see that

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

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

$f(x)$, $g(x)$ are coprime.
If $\deg \mathsf{GCD}(\hat{f}, \hat{g}) = k \Rightarrow \mathsf{rank}\, S(\hat{f}, \hat{g}) = m + n - k$. In our case $m = 13$, $n = 9$ and $k = 7$.

	$f(x)$	$g(x)$
x^{13}	1	
x^{12}	3.20025	
x^{11}	-8.26093	
x^{10}	-26.49540	
x^{9}	38.00476	1
x^{8}	85.59627	1.199981
x^{7}	-121.21627	-7.739988
x^{6}	-109.89824	-3.859967
x^{5}	223.97294	23.002372
x^{4}	-17.51887	-5.699975
x^{3}	-156.15339	-22.937378
x^{2}	120.28351	22.094884
x^{1}	-36.63814	-7.769948
x^{0}	4.14757	0.979989

	$\tilde{f}(x)$	$\tilde{g}(x)$
x^{13}	1	
x^{12}	3.19998	
x^{11}	-8.26007	
x^{10}	-26.49212	
x^{9}	38.00016	1
x^{8}	85.58606	1.199982
x^{7}	-121.20177	-7.739994
x^{6}	-109.88508	-3.859969
x^{5}	223.94605	23.002392
x^{4}	-17.51684	-5.699980
x^{3}	-156.13476	-22.937396
x^{2}	120.26907	22.094900
x^{1}	-36.63364	-7.769959
x^{0}	4.14719	0.979990

	$\mathrm{GCD}(\hat{f}, \hat{g})$	$\mathrm{GCD}(\tilde{f}, \tilde{g})$
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

4. Computing the GCD using c-s transformation

An example will be presented. Let

$$\begin{aligned} f(x) &= (x+3)^2(x+2.2)^2(x+0.5)^3(x-2)^4(x-3)^2 \\ g(x) &= (x+3.2)(x+3)^2(x+1.1)(x^2-0.01)(x-3)^2(x-4)^2. \end{aligned}$$

Denoting $u = \mathrm{GCD}(f, g)$, we have

$$u(x) = (x+3)^2(x-3)^2 = x^4 - 18x^2 + 81$$

Using FMLIB in our program we have obtained the exact result

$$\begin{aligned} \boldsymbol{u(x)} = \quad & \mathbf{1.000000000000000}\boldsymbol{x}^{\mathbf{4}} - \mathbf{18.000000000000000}\boldsymbol{x}^{\mathbf{2}} \\ & \mathbf{+81.000000000000000} \end{aligned}$$

The same example has been calculated in MatLab and the incorrect results have been obtained.

5. QR-factorization method for computing the greatest common divisor

A companion matrix associated with the polynomial f, where

$$f(x) = x^m + a_1 x^{m-1} + \cdots + a_{m-1}x + a_m,$$

is the $m \times m$ matrix

$$C_m = \begin{bmatrix} 0 & 1 & 0 & \dots & \dots & 0 \\ 0 & 0 & 1 & \dots & \dots & \vdots \\ \vdots & \vdots & \vdots & \dots & \dots & 1 \\ -a_m & -a_{m-1} & -a_{m-2} & \dots & -a_2 & -a_1 \end{bmatrix}.$$

It is assumed that the coefficient $a_0 = 1$. Now we will summarize the basic attributes of the matrix $g(C_m)$, where

$$g(x) = b_0 x^n + b_1 x^{n-1} + \cdots + b_{n-1}x + b_n,$$

in detail described in the Barnett's book. (S.Barnett: Polynomial and Linear Control System.)

Let $u = [b_n, b_{n-1}, \dots, b_1, b_0, 0, \dots, 0]^T \in \mathbb{R}^m$. Then the matrix polynomial $g(C_m)$ is given by

$$g(C_m) = \begin{bmatrix} u^T \\ u^T C_m \\ \vdots \\ u^T C_m^{m-2} \\ u^T C_m^{m-1} \end{bmatrix}.$$

The matrix $g(C_m)$ is very important.

The GCD(f, g) can be obtained very easily from the matrix $g(C_m)$.
Let us remark (S. Barnett) that

$$\deg(\mathrm{GCD}(f, g)) = m - \mathrm{rank}(g(C_m)).$$

Theorem 5.1 *Let $J_m \in \mathbb{R}^{m\times m}$ and $S(f, g)$ be matrices of the form*

$$J_m = [e_m, e_{m-1}, \dots, e_2, e_1] \quad \text{and} \quad S(f, g) = \begin{bmatrix} S_{1,1} & S_{1,2} \\ S_{2,1} & S_{2,2} \end{bmatrix},$$

where $S_{1,1} \in \mathbb{R}^{n\times n}$ *and* $S_{2,2} \in \mathbb{R}^{m\times m}$*. Then the Schur's complement*

$$S^*_{2,2} = J_m\, g(C_m) J_m.$$

The following idea (Barnett, Zarowski) will be illustrated for the polynomials of degree $m = 4$ and $n = 3$. Let

$$f(x) = x^4 + a_1 x^3 + a_2 x^3 + a_3 x + a_4 x,$$
$$g(x) = b_0 x^3 + b_1 x^2 + b_2 x + b_3.$$

Let the Sylvester matrix be split into the four blocks

$$\boldsymbol{S}(\boldsymbol{f},\boldsymbol{g}) =$$

$$= \left[\begin{array}{cccc|cccc} \mathbf{1} & \boldsymbol{a}_1 & \boldsymbol{a}_2 & & \boldsymbol{a}_3 & \boldsymbol{a}_4 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \boldsymbol{a}_1 & & \boldsymbol{a}_2 & \boldsymbol{a}_3 & \boldsymbol{a}_4 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & & \boldsymbol{a}_1 & \boldsymbol{a}_2 & \boldsymbol{a}_3 & \boldsymbol{a}_4 \\ \hline \boldsymbol{b}_0 & \boldsymbol{b}_1 & \boldsymbol{b}_2 & & \boldsymbol{b}_3 & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \boldsymbol{b}_0 & \boldsymbol{b}_1 & & \boldsymbol{b}_2 & \boldsymbol{b}_3 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \boldsymbol{b}_0 & & \boldsymbol{b}_1 & \boldsymbol{b}_2 & \boldsymbol{b}_3 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & & \boldsymbol{b}_0 & \boldsymbol{b}_1 & \boldsymbol{b}_2 & \boldsymbol{b}_3 \end{array}\right] =: \left[\begin{array}{cc} \boldsymbol{S}_{1,1} & \boldsymbol{S}_{1,2} \\ \boldsymbol{S}_{2,1} & \boldsymbol{S}_{2,2} \end{array}\right]$$

It is clear that all blocks are Toeplitz matrices. The Schur complement follows from the following multiplication:

$$\left[\begin{array}{cc} \boldsymbol{I}_3 & \mathbf{0} \\ -\boldsymbol{S}_{2,1}\boldsymbol{S}_{1,1}^{-1} & \boldsymbol{I}_4 \end{array}\right] \left[\begin{array}{cc} \boldsymbol{S}_{1,1} & \boldsymbol{S}_{1,2} \\ \boldsymbol{S}_{2,1} & \boldsymbol{S}_{2,2} \end{array}\right] = \left[\begin{array}{cc} \boldsymbol{S}_{1,1} & \boldsymbol{S}_{1,2} \\ \mathbf{0} & \boldsymbol{S}_{2,2}^{(*)} \end{array}\right],$$

where

$$\boldsymbol{S}_{2,2}^{(*)} = \boldsymbol{S}_{2,2} - \boldsymbol{S}_{2,1}\boldsymbol{S}_{1,1}^{-1}\boldsymbol{S}_{1,2}$$

Theorem 5.2.[Barnett and Zarowski] *There exist square matrices U and Q such that*

$$\begin{aligned} US(f,g) &= R_1, \\ QS^*_{2,2} &= R_2, \end{aligned}$$

where R_1 and R_2 are upper triangular matrices. The last non-vanishing rows of both triangular matrices contain the coefficients of a GCD(f,g).

Moreover, there is an orthogonal matrix Q such that

$$QJ_m g(C_m) J_m = R_2$$

[Zarowski], where

$$
R = \begin{bmatrix}
x & x & . & . & x & x & x & . & . & x & x \\
0 & x & . & . & x & x & x & . & . & x & x \\
. & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & . \\
0 & 0 & . & . & x & x & x & . & . & x & x \\
0 & 0 & . & . & 0 & d_0 & d_1 & . & . & d_{k-1} & d_k \\
0 & 0 & . & . & 0 & 0 & 0 & . & . & 0 & 0 \\
. & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & . \\
0 & 0 & . & . & 0 & 0 & 0 & . & . & 0 & 0
\end{bmatrix},
$$

and $d(x) := d_0 x^k + d_1 x^{k-1} + \cdots + d_{k-1} x + d_k$ is the GCD of f and g. $\square$

An example: the same polynomials are considered, i.e.,

$$
\begin{aligned}
f(x) &= (x+3)^2(x+2.2)^2(x+0.5)^3(x-2)^4(x-3)^2 \\
g(x) &= (x+3.2)(x+3)^2(x+1.1)(x^2-0.01)(x-3)^2(x-4)^2.
\end{aligned}
$$

Let us remark that $u = \mathrm{GCD}(f, g)$,

$$u(x) = (x+3)^2(x-3)^2 = x^4 - 18x^2 + 81.$$

We have obtained again the exact result. The same example was calculated in MatLab and the polynomial p has been obtained.

$$\begin{aligned} p(x) = \quad & 1.000000000000000x^4 - 0.000000141260423x^3 \\ & -17.999999475530075x^2 + 0.000000973322225x \\ & +80.999996276344888 \end{aligned}$$

The Euclidean norm $\|p - u\| = 3.886899375985486e - 6$.

The second approach to construction of $g(C_m)$ was based on direct computing of Schur's complement $S^*_{2,2}$. We have obtained the polynomial p such that

$$\begin{aligned} p(x) = \quad & 1.000000000000000x^4 + 0.000001622363975x^3 \\ & -17.999998869020878x^2 - 0.000012113435782x \\ & +80.999991505224259 \end{aligned}$$

The Euclidean norm $\|p - u\| = 1.492674512347724e-5$. At the end of this lecture we will present an interesting example.

Let

$$\begin{aligned} f(x) &= \prod_{i \in N_1} (x - i) \\ g(x) &= \prod_{i \in N_2} (x - i), \end{aligned}$$

where $N_1 = \{1, 2, \ldots, 20\}$,
$N_2 = \{1, 2, \ldots, 10\} \cup \{-1, -2, -3, -4\}$

In this case we have again obtained the exact solution.

The End

Thank you for your attention!