Solving Polynomial Systems
Using Subresultants

Grant McNaughton

28 April 2024

In this paper, we will develop mathematical theories and algorithms for the following problem.

Input: $f \in \mathbb{C}[x_1, \ldots, x_n]^n$

Output: $S = V(f)$, the set of all complex solutions of f.

1 Theory

Notation 1 *Let*

$$\begin{aligned} f &= a_p x^p + \cdots + a_0 x^0 \\ g &= b_q x^q + \cdots + b_0 x^0 \end{aligned}$$

where x is a variable and a_i and b_i are coefficients which might be again polynomials in other variables.

Definition 2 (Subresultant) *The k-th subresultant of f and g with respect to x, written as $R_{x,k}(f, g)$, is defined by*

$$\begin{vmatrix}
a_p & a_{p-1} & \cdots & a_{\epsilon+1} & a_\epsilon & a_{\epsilon-1} & \cdots & a_{2k-q+2} & a_{2k-q+1}x^k + \cdots + a_0 x^{q-k-1} \\
0 & a_p & \cdots & a_{\epsilon+2} & a_{\epsilon+1} & a_\epsilon & \cdots & a_{2k-q+3} & a_{2k-q+2}x^k + \cdots + a_0 x^{q-k-2} \\
\vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\
0 & 0 & \cdots & a_{\delta+1} & a_\delta & a_{\delta-1} & \cdots & a_{2k+q+r+1} & \sum_{n=0}^{2k-q+r} a_n x^{n+q-k-r} \\
\vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\
0 & 0 & \cdots & a_p & a_{p-1} & a_{p-2} & \cdots & a_k & a_{k-1}x^k + \cdots + a_0 x^1 \\
0 & 0 & \cdots & 0 & a_p & a_{p-1} & \cdots & a_{k+1} & a_k x^k + \cdots + a_0 x^0 \\
b_q & b_{q-1} & \cdots & b_{\epsilon+1} & b_\epsilon & b_{\epsilon-1} & \cdots & b_{2k-p+2} & b_{2k-p+1}x^k + \cdots + b_0 x^{p-k-1} \\
0 & b_q & \cdots & b_{\epsilon+2} & b_{\epsilon+1} & b_\epsilon & \cdots & b_{2k-p+3} & b_{2k-q+2}x^k + \cdots + b_0 x^{p-k-2} \\
\vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\
0 & 0 & \cdots & b_{\delta+1} & b_\delta & b_{\delta-1} & \cdots & b_{3k-p-q+r+1} & \sum_{n=1}^{3k-p-q+r} b_n x^{n-2k+p+q-r} \\
\vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\
0 & 0 & \cdots & b_q & b_{q-1} & b_{q-2} & \cdots & b_k & b_{k-1}x^k + \cdots + b_0 x^1 \\
0 & 0 & \cdots & 0 & b_q & b_{q-1} & \cdots & b_{k+1} & b_k x^k + \cdots + b_0 x^0
\end{vmatrix}$$

where r is given by the row number, starting at 1 and ending at $q+p-2k$. The matrix defining the subresultant is in $\mathbb{R}^{q+p-2k \times q+p-2k}$.

Theorem 3 *We have*

1. $\deg_x R_{x,k} \leq k$
2. $R_{x,k}(f,g) \in \langle f,g \rangle$.

Proof.

1. Obvious from Laplace expansion along the last column.
2. For the sake of simple presentation, we show the proof only for $p=3,\ q=4$ and $k=1$.

   Note that $f = a_3x^3 + a_2x^2 + a_1x + a_0$ and $g = b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$ and that we can define $R_{x,1}(f,g)$ as

   $$\begin{vmatrix} a_3 & a_2 & a_1 & a_0 & 0 \\ 0 & a_3 & a_2 & a_1 & a_0x \\ 0 & 0 & a_3 & a_2 & a_1x + a_0 \\ b_4 & b_3 & b_2 & b_1 & b_0x \\ 0 & b_4 & b_3 & b_2 & b_1x + b_0 \end{vmatrix}$$

   This matrix is 5×5 and we will define its columns as c_1, c_2, c_3, c_4, and c_5 respectively. Using determinant rules, we can redefine c_5 as $c_5 + c_4x^2 + c_3x^3 + c_2x^4 + c_1x^5$ without changing the determinant of the matrix. Thus

   $$\begin{vmatrix} a_3 & a_2 & a_1 & a_0 & 0 \\ 0 & a_3 & a_2 & a_1 & a_0x \\ 0 & 0 & a_3 & a_2 & a_1x + a_0 \\ b_4 & b_3 & b_2 & b_1 & b_0x \\ 0 & b_4 & b_3 & b_2 & b_1x + b_0 \end{vmatrix} = \begin{vmatrix} a_3 & a_2 & a_1 & a_0 & a_0x^2 + a_1x^3 + a_2x^4 + a_3x^5 \\ 0 & a_3 & a_2 & a_1 & a_0x + a_1x^2 + a_2x^3 + a_3x^4 \\ 0 & 0 & a_3 & a_2 & a_0 + a_1x + a_2x^2 + a_3x^3 \\ b_4 & b_3 & b_2 & b_1 & b_0x + b_1x^2 + b_2x^3 + b_3x^4 + b_4x^5 \\ 0 & b_4 & b_3 & b_2 & b_0 + b_1x + b_2x^2 + b_3x^3 + b_4x^4 \end{vmatrix}$$

   $$= \begin{vmatrix} a_3 & a_2 & a_1 & a_0 & x^2f \\ 0 & a_3 & a_2 & a_1 & xf \\ 0 & 0 & a_3 & a_2 & f \\ b_4 & b_3 & b_2 & b_1 & xg \\ 0 & b_4 & b_3 & b_2 & g \end{vmatrix} = \begin{vmatrix} a_3 & a_2 & a_1 & a_0 & x^2f \\ 0 & a_3 & a_2 & a_1 & xf \\ 0 & 0 & a_3 & a_2 & f \\ b_4 & b_3 & b_2 & b_1 & 0 \\ 0 & b_4 & b_3 & b_2 & 0 \end{vmatrix} + \begin{vmatrix} a_3 & a_2 & a_1 & a_0 & 0 \\ 0 & a_3 & a_2 & a_1 & 0 \\ 0 & 0 & a_3 & a_2 & 0 \\ b_4 & b_3 & b_2 & b_1 & xg \\ 0 & b_4 & b_3 & b_2 & g \end{vmatrix}$$

   We can then use determinant rules to factor out f and g from c_5, giving

   $$\begin{vmatrix} a_3 & a_2 & a_1 & a_0 & x^2 \\ 0 & a_3 & a_2 & a_1 & x \\ 0 & 0 & a_3 & a_2 & 1 \\ b_4 & b_3 & b_2 & b_1 & 0 \\ 0 & b_4 & b_3 & b_2 & 0 \end{vmatrix} f + \begin{vmatrix} a_3 & a_2 & a_1 & a_0 & 0 \\ 0 & a_3 & a_2 & a_1 & 0 \\ 0 & 0 & a_3 & a_2 & 0 \\ b_4 & b_3 & b_2 & b_1 & x \\ 0 & b_4 & b_3 & b_2 & 1 \end{vmatrix} g$$

   If we set $U(x) = \begin{vmatrix} a_3 & a_2 & a_1 & a_0 & x^2 \\ 0 & a_3 & a_2 & a_1 & x \\ 0 & 0 & a_3 & a_2 & 1 \\ b_4 & b_3 & b_2 & b_1 & 0 \\ 0 & b_4 & b_3 & b_2 & 0 \end{vmatrix}$ and $V(x) = \begin{vmatrix} a_3 & a_2 & a_1 & a_0 & 0 \\ 0 & a_3 & a_2 & a_1 & 0 \\ 0 & 0 & a_3 & a_2 & 0 \\ b_4 & b_3 & b_2 & b_1 & x \\ 0 & b_4 & b_3 & b_2 & 1 \end{vmatrix}$, then we can say that $R_{x,1}(f,g) = U(x)f + V(x)g$, thus $R_{x,1}(f,g) \in \langle f,g \rangle$

■

Definition 4 (Triangularization) *Let*

$$f = (f_1, \ldots, f_n) \in \mathbb{C}[x_1, \ldots, x_n]^n.$$

Then the triangularization *of f, denoted as*

$$\tilde{f} = \left(\tilde{f}_1, \ldots, \tilde{f}_n\right) \in \mathbb{C}[x_1, \ldots, x_n]^n$$

is defined by the following process.

(For the sake of simple presentation, we will show the $n = 4$ case only. The generalization to arbitrary n is straightforward).

1. *Repeated* 0*-th order subresultant (resultant):*

$$\begin{array}{llll} f_1 & & & \\ f_2 & f_{12} = R_{x_1,0}\left(f_1, f_2\right) & & \\ f_3 & f_{13} = R_{x_1,0}\left(f_1, f_3\right) & f_{123} = R_{x_2,0}\left(f_{12}, f_{13}\right) & \\ f_4 & f_{14} = R_{x_1,0}\left(f_1, f_4\right) & f_{124} = R_{x_2,0}\left(f_{12}, f_{14}\right) & f_{1234} = R_{x_3,0}\left(f_{123}, f_{124}\right) \end{array}$$

2. 1*-st order subresultant:*

$$\begin{aligned} \tilde{f}_1 &= R_{x_1,1}\left(f_1, f_2\right) \\ \tilde{f}_2 &= R_{x_2,1}\left(f_{12}, f_{13}\right) \\ \tilde{f}_3 &= R_{x_3,1}\left(f_{123}, f_{124}\right) \\ \tilde{f}_4 &= f_{1234} \end{aligned}$$

Theorem 5 $V(\tilde{f}) \supseteq V(f)$

Proof. For the sake of simple presentation, we show the proof only for $n = 4$. We will first show that $\tilde{f}_1, \tilde{f}_2, \tilde{f}_3, \tilde{f}_4 \in \langle f_1, f_2, f_3, f_4 \rangle$, then we will use that to show that for any $\alpha \in V(f)$, $\alpha \in V(\tilde{f})$ as well.

Note the following:

$$\tilde{f}_1 = R_{x_1,1}(f_1, f_2) \in \langle f_1, f_2 \rangle \subset \langle f_1, f_2, f_3, f_4 \rangle$$

$$\begin{aligned} \tilde{f}_2 &= R_{x_2,1}\left(f_{12}, f_{13}\right) \in \langle f_{12}, f_{13} \rangle = \langle R_{x_1,0}\left(f_1, f_2\right), R_{x_1,0}\left(f_1, f_3\right) \rangle \\ &\subset \langle \langle f_1, f_2 \rangle, \langle f_1, f_3 \rangle \rangle \subset \langle f_1, f_2, f_3 \rangle \subset \langle f_1, f_2, f_3, f_4 \rangle \end{aligned}$$

$$\begin{aligned} \tilde{f}_3 &= R_{x_3,1}\left(f_{123}, f_{124}\right) \in \langle f_{123}, f_{123} \rangle = \langle R_{x_2,0}(f_{12}, f_{13}), R_{x_2,0}(f_{12}, f_{14}) \rangle \\ &\subset \langle \langle f_{12}, f_{13} \rangle, \langle f_{12}, f_{14} \rangle \rangle \subset \langle f_{12}, f_{13}, f_{14} \rangle = \langle R_{x_1,0}(f_1, f_2), R_{x_1,0}(f_1, f_3), R_{x_1,0}(f_1, f_4) \rangle \\ &\subset \langle \langle f_1, f_2 \rangle, \langle f_1, f_3 \rangle, \langle f_1, f_4 \rangle \rangle \subset \langle f_1, f_2, f_3, f_4 \rangle \end{aligned}$$

$$\tilde{f}_4 = R_{x_3,0}\left(f_{123}, f_{124}\right) \in \langle f_{123}, f_{124} \rangle \subset \langle f_1, f_2, f_3, f_4 \rangle$$

Thus $\tilde{f} \in \langle f \rangle$. Because of this, we can define $\tilde{f}$ as follows:

$$\begin{aligned} \tilde{f}_1 &= u_{11} f_1 + u_{12} f_2 + u_{13} f_3 + u_{14} f_4 \\ \tilde{f}_2 &= u_{21} f_1 + u_{22} f_2 + u_{23} f_3 + u_{24} f_4 \\ \tilde{f}_3 &= u_{31} f_1 + u_{32} f_2 + u_{33} f_3 + u_{34} f_4 \\ \tilde{f}_4 &= u_{41} f_1 + u_{42} f_2 + u_{43} f_3 + u_{44} f_4 \end{aligned}$$

for some set of u's in $\mathbb{R}$. Let α solve f, that is $f_1(\alpha) = f_2(\alpha) = f_3(\alpha) = f_4(\alpha) = 0$. From this, we can say that $\tilde{f}_1(\alpha) = u_{11} \cdot 0 + u_{12} \cdot 0 + u_{13} \cdot 0 + u_{14} \cdot 0 = 0$, which is similarly true for $\tilde{f}_2$, $\tilde{f}_3$, and $\tilde{f}_4$. Because $\tilde{f}_1(\alpha) = \tilde{f}_2(\alpha) = \tilde{f}_3(\alpha) = \tilde{f}_4(\alpha) = 0$, we know that $\alpha \in V(\tilde{f})$. Therefore it must be true that $V(f) \subseteq F(\tilde{f})$.
■

2 Algorithms

Algorithm 6 (Triangularize)

1. $h \leftarrow f$
2. $\tilde{f} \leftarrow 0_{n\times 1}$
3. *For* $i = 0, \ldots, n-1$

   $\tilde{f}_i \leftarrow R_{x_i,1}(h_i, h_{i+1})$

   where for $j = i+1, \ldots, n-1$

   $h_j \leftarrow R_{x_i,0}(h_i, h_j)$
4. $\tilde{f}_n \leftarrow h_{n-1}$

Algorithm 7 (BackSubstitute)

1. $rs \leftarrow$ *All complex roots of* $\tilde{f}_{n-1}$
2. $T \leftarrow [\ ]$*, an empty list*
3. *For a root* r *in* rs,

   $t \leftarrow 0_{n\times 1}$

   $t_{n-1} \leftarrow r$

   where for $i = n-2, n-1, \ldots, 1, 0$

   where for $j = i+1, \ldots, n-1$

   $h \leftarrow \tilde{f}_i(t_j)$

   $t_i \leftarrow -\frac{coeff(h,x_i,0)}{coeff(h,x_i,1)}$*, where the coefficients are evaluated on* h *at* x_i^0 *and* x_i^1

   Append t *to* T
4. $T \leftarrow$ *All possible complex solutions to* $\tilde{f}$

Algorithm 8 (ChooseSolution)

1. $S \leftarrow [\ ]$*, an empty list*
2. *For a solution* t *in* T,

   $h \leftarrow f(t)$

   and if $||h||_2 \leq \epsilon$*, append* h *to* S
3. $S \leftarrow$ *All possible complex solutions to* f