J. Inst. Maths Applics (1978) **22**, 331–335

Generalized Resultant Theorem

A. I. G. VARDULAKIS AND P. N. R. STOYLE
Department of Computing and Control, Imperial College, London SW7 2AZ

[Received 15 February 1978]

The classical resultant theorem regarding the relative primeness of two polynomials is generalized for m ($m \geqslant 2$) polynomials.

1. Introduction

A CLASSICAL theorem by Sylvester states that two polynomials are relatively prime if and only if their resultant matrix is non-singular (Wolovich, 1974).

The relative primeness of several polynomials was investigated by Van Der Waerden (1949). These results are however more of theoretical importance and do not provide us directly with a simple numerical test for the relative primeness of m ($m \geqslant 2$) polynomials.

Barnett (1971) investigated the same problem and gave a test for relative primeness of m polynomials in terms of the rank of a matrix. The formation of the Barnett matrix from the coefficients of the m polynomials necessitates some computation, e.g. multiplications of vectors by matrices (Barnett, 1971, Section 4) and its structure does not represent a direct generalization of the classical resultant matrix for two polynomials.

In this paper a direct generalization of the classical resultant theorem is established. It is shown that a necessary and sufficient condition for m polynomials to be relatively prime is that a certain matrix, which can be formed very easily by a special arrangement of the coefficients of the m polynomials, must have full rank.

In the following we let $\mathbf{m}$ denote the set of integers $\{1, 2, \ldots, m\}$.

2. Generalized Resultant Matrix

Consider m ($m \geqslant 2$) polynomials with coefficients in the real field $\mathbb{R}$

$$b_i(s) = b_{i0} + b_{i1}s + \ldots + b_{in}s^n, \quad i \in \mathbf{m}, \tag{1}$$

such that for some $i \in \mathbf{m}$, $b_{in} \neq 0$ (i.e. at least one of the polynomials is of degree n), let

0020-2932/78/070331+05 $02.00/0

$S(s)$ be the $nm \times m$ matrix

$$S(s) = \left[\begin{array}{cccc} 1 & 0 & \dots & 0 \\ s & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ s^{n-1} & 0 & \dots & 0 \\ \hline 0 & 1 & \dots & 0 \\ 0 & s & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & s^{n-1} & & 0 \\ \hline 0 & 0 & \dots & 1 \\ 0 & 0 & \dots & s \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & s^{n-1} \end{array}\right] \tag{2}$$

and define

$$x(s) \triangleq S(s) \begin{bmatrix} b_1(s) \\ b_2(s) \\ \vdots \\ b_m(s) \end{bmatrix} = \left[\begin{array}{c} b_1(s) \\ sb_1(s) \\ \vdots \\ s^{n-1}b_1(s) \\ \hline \vdots \\ \hline b_m(s) \\ sb_m(s) \\ \vdots \\ s^{n-1}b_m(s) \end{array}\right] = x_0 + x_1 s + \dots + x_{2n-1}s^{2n-1}$$

$$= (x_0, x_1, \dots, x_{2n-1}) \begin{bmatrix} 1 \\ s \\ s^2 \\ \vdots \\ s^{2n-1} \end{bmatrix} = R\hat{s}. \tag{3}$$

Then it can be verified that $R = (x_0, x_1, \ldots, x_{2n-1})$ is a $nm \times 2n$ matrix having the form:

$$R = \left[\begin{array}{cccccccc}
b_{10} & b_{11} & \cdots & & b_{1n} & 0 & \cdots & 0 \\
0 & b_{10} & \cdots & & b_{1,n-1} & b_{1n} & \cdots & 0 \\
\vdots & \vdots & & & \vdots & \vdots & & \vdots \\
0 & 0 & \cdots & b_{10} & b_{11} & b_{12} & \cdots & b_{1n} \\
\hline
b_{20} & b_{21} & \cdots & & b_{2n} & 0 & \cdots & 0 \\
0 & b_{20} & \cdots & & b_{2,n-1} & b_{2n} & \cdots & 0 \\
\vdots & \vdots & & & \vdots & \vdots & & \vdots \\
0 & 0 & \cdots & b_{20} & b_{21} & b_{22} & \cdots & b_{2n} \\
\hline
\vdots & & & & & & & \\
\hline
b_{m0} & b_{m1} & \cdots & & b_{mn} & 0 & \cdots & 0 \\
0 & b_{m0} & \cdots & & b_{m,n-1} & b_{mn} & \cdots & 0 \\
\vdots & \vdots & & & \vdots & \vdots & & \vdots \\
0 & 0 & \cdots & b_{m0} & b_{m1} & b_{m2} & \cdots & b_{mn}
\end{array}\right] = \left[\begin{array}{c} R_1 \\ \hline R_2 \\ \hline \vdots \\ \hline R_m \end{array}\right]. \quad (4)$$

We call R the generalized resultant matrix for the m polynomials $b_i(s)$, $i \in \mathbf{m}$. We can now state the following.

THEOREM. *A necessary and sufficient condition for the m polynomials $b_i(s)$, $i \in \mathbf{m}$, to be relatively prime is that rank $R = 2n$.*

Proof. ($b_i(s)$, $i \in \mathbf{m}$, have common factor $\Rightarrow$ rank $R < 2n$.) Assume that the $b_i(s)$, $i \in \mathbf{m}$, have some non-trivial polynomial common factor $a(s)$ of deg. $a(s) > 0$, i.e. assume that the polynomials can be written as: $b_i(s) = a(s)b_i'(s)$, $i \in \mathbf{m}$, where $b_i'(s)$, $i \in \mathbf{m}$, are such that g.c.d. $\{b_i'(s),\ i \in \mathbf{m}\} = 1$ and let $\lambda \in \mathbb{C}$ be some zero of $a(s)$.

Then

$$x(\lambda) = a(\lambda)S(\lambda)\begin{bmatrix} b_1'(\lambda) \\ b_2'(\lambda) \\ \vdots \\ b_m'(\lambda) \end{bmatrix} = x_0 + x_1\lambda + \ldots + x_{2n-1}\lambda^{2n-1} = 0,$$

i.e. the $2n$ vectors $x_0, x_1, \ldots, x_{2n-1}$ are linearly dependent (over C) and hence rank $R < 2n$. (Conversely, rank $R < 2n \Rightarrow b_i(s)$, $i \in \mathbf{m}$, have some non-trivial common factor.) In order to prove this we need the following:

LEMMA. *In order that a polynomial $a(s)$ is a common factor of the polynomials $b_1(s)$, $b_2(s), \ldots, b_m(s)$ it is necessary and sufficient that it is a common factor of $b_1(s)$ and*

$$b_k(s) = \sum_{i=2}^{m} k_i b_i(s),$$

where $k_2, k_3, \ldots, k_m$ represent $m-1$ indeterminates. (Van-der-Waerden, 1949, Chapter 11, Section 77, see also Remarks, 1.)

Now, returning to the proof of the theorem, we have by assumption that rank $R < 2n$ and with the indeterminates $k_2, k_3, \ldots, k_m$:

$$\text{rank } R = \text{rank} \begin{bmatrix} R_1 \\ \hline k_2R_2 + k_3R_3 + \ldots + k_mR_m \\ \hline \vdots \\ \hline R_m \end{bmatrix} = \text{rank } R' < 2n$$

(Gantmacher (1960), Theorem 3, p. 45). The above implies that all $2n$-order minors of R' are equal to zero, and in particular that

$$\det \begin{bmatrix} R_1 \\ \hline \sum_{i=2}^{m} k_iR_i \end{bmatrix} = 0$$

which, by the classical resultant theorem, implies that $b_1(s)$ and $b_k(s)$ have a common factor and, by the above lemma, that the polynomials $b_i(s)$, $i \in \mathbf{m}$ have the same common factor. Q.E.D.

If $a(s)$ is the g.c.d. of the $b_i(s)$, $i \in \mathbf{m}$ then, from the lemma, $a(s)$ is also the g.c.d. of $b_1(s)$ and $b_k(s)$, and

$$\deg a(s) = n - \text{rank } R' = n - \text{rank } R.$$

So we have the following.

COROLLARY. *The degree of the greatest common devisor $a(s)$ of the polynomials $b_i(s)$, $i \in \mathbf{m}$, is equal to the rank defect of R, i.e.*

$$\deg a(s) = 2n - \text{rank } R.$$

3. Conclusion

The generalized resultant matrix appeared originally in our investigation of the structure and the polynomial parametrization of the family of controllability subspaces that correspond to a matrix pair (A, B) describing the state space model data of a linear multi-input system (Vardulakis, 1977).

As the concept of controllability subspaces of (A, B) plays an important role in the modern "geometric approach" theory of linear multivariable systems, it is hoped that the theorem presented here, apart from its own mathematical importance, will clarify some of the nice algebraic properties of controllability subspaces (Stoyle & Vardulakis, 1978).

A. I. G. Vardulakis would like to thank the U.K. Science Research Council for financial support.

References

Barnett, S. 1971 *Proc. Camb. Phil. Soc.* **70**, 263–268.

Gantmacher, F. R. 1960 *The Theory of Matrices*, Vol. I. New York: Chelsea Publ. Co.

Stoyle, P. N. R. & Vardulakis, A. I. G. 1978 *CCD Research Report No. 78/2*. Imperial College, also to appear in the *Int. J. Control.*

Van Der Waerden, 1949 *Modern Algebra*, Vol. II. New York: Frederic Ungar Publ. Co.

Vardulakis, A. I. G. 1977 *CCD Research Report No. 77/10*. Imperial College, also to appear in the *Int. J. Control.*

Wolovich, W. A. 1974 *Linear Multivariable Systems*. Berlin: Springer-Verlag.