Structure of a Class of Unimodular Matrices*

Brian D. O. Anderson

Department of Electrical Engineering
University of Newcastle
New South Wales, 2308, Australia

Submitted by Hans Schneider

ABSTRACT

A decomposition theorem is established for square matrices $A(s)$ defined over $R[s]$, the ring of real polynomials in a variable s, which satisfy the condition $A(s)A(-s)=I$.

1. INTRODUCTION

We shall be concerned with square matrices defined over the ring $R[s]$ of real polynomials in a single indeterminate s. A matrix over $R[s]$ is unimodular if and only if its determinant is a nonzero real constant, i.e., if and only if its inverse is also a matrix over $R[s]$. In this paper, we shall prove a structural result concerning unimodular matrices $A(s)$ with the property that $A(s)A(-s)=I$. We came upon the need for this result in examining several problems of linear system theory with the aid of polynomial matrices; we mention a single linear system theory application of the result later in this paper.

2. MAIN RESULT

Unless otherwise specified, all matrices are defined over $R[s]$.

THEOREM 1. *Let $A(s)$ be an $n\times n$ matrix. Then $A(s)A(-s)=I$ if and only if there exist a unimodular matrix $U(s)$ and a signature matrix Σ (i.e., a*

*Work supported by the Australian Research Grants Committee.

0024-3795/78/0022-0167$01.25

diagonal matrix with only ± 1 *diagonal elements) such that*

$$A(s) = U(s)\Sigma U^{-1}(-s). \tag{1}$$

If (1) holds with unimodular $U(s)$, it is trivial to conclude that $A(s)A(-s) = I$. So our task is to exhibit (1) in case $A(s)A(-s) = I$.

3. PROOF OF MAIN RESULT

We shall proceed via a series of lemmas, some of which involve properties of the matrix

$$B(s) = \begin{bmatrix} 0 & A(-s) \\ A(s) & 0 \end{bmatrix}. \tag{2}$$

We shall also make use of the Hermite form of a square polynomial matrix [1,2]. For arbitrary square $X(s)$ there exist a unimodular $Y(s)$ and a unique lower triangular $Z(s)$, the Hermite form of $X(s)$, with monic diagonal entries and such that the polynomial degree $\delta[z_{ji}(s)]$ of $z_{ji}(s)$ is less than $\delta[z_{ii}]$ for $j > i$. Further,

$$X(s) = Y(s)Z(s). \tag{3}$$

[By considering the Hermite form of $X'(s)$, the transpose of $X(s)$, we can get a similar decomposition of $X(s)$ as $Z(s)Y(s)$ with $Z(s)$ upper triangular and $\delta[z_{ii}] > \delta[z_{ij}]$ for $j > i$.]

LEMMA 1. *If* $A(s)A(-s) = I$, *there exist a* $2n \times 2n$ *nonsingular matrix* $C(s)$ *and a* $2n \times 2n$ *signature matrix* Σ *such that*

$$B(s)C(s) = C(s)\Sigma. \tag{4}$$

Proof. From $A(s)A(-s) = I$, it easily follows that $B^2(s) - I = 0$. Since neither $B - I = 0$ nor $B + I = 0$, $x^2 - 1$ is the minimum polynomial of B. Since this polynomial has no repeated roots, $B(s)$ for each fixed s is diagonalizable over R. Thus (4) holds, if we do not require $C(s)$ to be over $R[s]$.

The remainder of the proof is concerned with the technical issue of exhibiting (4) with $C(s)$ a matrix over $R[s]$.

Define $\nu_{\pm}(s_0)=\text{nullity}(B(s_0)\pm I)$ for each fixed s_0, and $\nu_{\pm}=\text{nullity}(B(s)\pm I)$, where $\text{rank}(B(s)\pm I)$ is the size of the largest minor of $B(s)\pm I$ which is not identically zero in s. Because of the diagonalizability of $B(s_0)$ and the fact that the only eigenvalues of $B(s_0)$ are ± 1, one has for each fixed s_0

$$\nu_{+}(s_0)+\nu_{-}(s_0)=2n.$$

Further, it is clear that the same equation for the nullities $\nu_{\pm}$ holds, while also $\nu_{+}\geqslant\nu_{+}(s_0)$, $\nu_{-}\geqslant\nu_{-}(s_0)$ for all s_0. It follows that $\nu_{+}(s_0)=\nu_{+}$, $\nu_{-}(s_0)=\nu_{-}$ for all s_0. By elementary column transformations over $R[s]$, we can then find a matrix $\Gamma_{+}(s)$ over $R[s]$ such that

$$[B(s)+I]\Gamma_{+}(s)=[x \quad \cdots \quad x \,\vdots\, 0 \quad \cdots \quad 0]$$

with the number of zero columns equal to ν_{+}. Define the last ν_{+} columns of $\Gamma_{+}(s)$ as $c_1(s),\dots,c_{\nu_+}(s)$. Then

$$[B(s)+I][\, c_1(s) \quad \cdots \quad c_{\nu_+}(s)\,]=0$$

with $c_i(s)\in R[s]$ and with $c_1(s),\dots,c_{\nu_+}(s)$ linearly independent. Similarly, we can find $c_{\nu_+ +1}(s),\dots,c_{2n}(s)\in R[s]$ and linearly independent with

$$[B(s)-I][\, c_{\nu_+ +1}(s) \quad \cdots \quad c_{2n}(s)\,]=0.$$

It is easily checked that $c_1(s),\dots,c_{2n}(s)$ form a linearly independent set and so

$$B(s)C(s)=C(s)\Sigma,$$

where $C(s)=[c_1(s) \quad \cdots \quad c_{2n}(s)]$. ■

In the next lemma, we impose some structure on $C(s)$.

Lemma 2. *Without loss of generality, the matrix $C(s)$ in Lemma* 1 *may be taken to have the form*

$$D(s)=\begin{bmatrix} d_1(s) & d_2(s) & \cdots & d_{2n}(s) \\ \pm d_1(-s) & \pm d_2(-s) & \cdots & \pm d_{2n}(-s) \end{bmatrix}.$$

Proof. Suppose that

$$B(s)\begin{bmatrix} u(s) \\ v(s) \end{bmatrix} = \varepsilon \begin{bmatrix} u(s) \\ v(s) \end{bmatrix}$$

with $u(s), v(s)$ n-vectors in $R[s]$ and $\varepsilon = +1$ or -1. Then the form of B easily implies that

$$B(s)\begin{bmatrix} v(-s) \\ u(-s) \end{bmatrix} = \varepsilon \begin{bmatrix} v(-s) \\ u(-s) \end{bmatrix}.$$

Thus if $[\, u'(s) \quad v'(s) \,]'$ is an eigenvector, so are $[\, e'(s) \quad e'(-s) \,]'$ and $[\, f'(s) \quad -f'(-s) \,]'$, where $e(s) = u(s) + v(-s)$ and $f(s) = u(s) - v(-s)$. Note that one, but not both, of e and f may be zero.

The ith column of the matrix $C(s)$ in (4) as an eigenvector of $B(s)$ gives rise to two further vectors $[\, e_i'(s) \quad e_i'(-s) \,]'$ and $[\, f_i'(s) \quad -f_i'(-s) \,]'$, which if nonzero are eigenvectors of $B(s)$. The resulting set of $4n$ column vectors spans the $2n$ columns of C. The set therefore contains $2n$ linearly independent vectors, which we shall write as $[\, d_1'(s) \quad \pm d_1'(-s) \,]', [\, d_{2n}'(s) \quad \pm d_{2n}'(-s) \,]'$, each of which is an eigenvector of $B(s)$. This proves the result. ■

Next, we can secure the result (1) without the requirement that $U(s)$ should be unimodular. Thus $U^{-1}(-s)$ may not be over $R[s]$, but will be rational.

LEMMA 3. *With $A(s)$ polynomial and such that $A(s)A(-s) = I$, there exists a $U(s)$ such that* (1) *holds.*

Proof. Let $D(s)$ be as in the statement of Lemma 2. Since $D(s)$ is of full rank, the first n rows are linearly independent. Hence there exist n columns in the first n rows such that the resulting $n \times n$ matrix is nonsingular. Without loss of generality, we may rearrange the columns of $D(s)$ so that these n columns occur first. Therefore

$$\begin{bmatrix} 0 & A(-s) \\ A(s) & 0 \end{bmatrix} \begin{bmatrix} d_1(s) & \cdots & d_n(s) \\ \pm d_1(-s) & \cdots & \pm d_n(-s) \end{bmatrix}$$

$$= \begin{bmatrix} d_1(s) & \cdots & d_n(s) \\ \pm d_1(-s) & \cdots & \pm d_n(-s) \end{bmatrix} \Sigma,$$

where Σ is now an $n\times n$ signature matrix. From this, we have

$$\begin{aligned} A(s)[\,d_1(s) \quad \cdots \quad d_n(s)\,] &= [\,\pm d_1(-s) \quad \cdots \quad \pm d_n(-s)\,]\Sigma \\ &= [\,d_1(-s) \quad \cdots \quad d_n(-s)\,]\bar{\Sigma} \end{aligned}$$

for some new signature matrix $\bar{\Sigma}$. Now drop the overbar and set $U(s)=[d_1(-s) \ \cdots \ d_n(-s)]$ to obtain (1). ∎

In order to complete this proof of the theorem, we must show that $U(s)$ can be taken to be unimodular. The next lemma in effect explains how one may pass from a decomposition of the form (1) with $U(s)$ not unimodular to a further decomposition incorporating the unimodular constraint. Notice that if $A(s)$ over $R[s]$ has the form (1) with $U(s)$ not unimodular, $A(s)$ must still be unimodular, since $A(s)$ has an inverse over $R[s]$, viz $A(-s)$.

LEMMA 4. *Let $A(s)=U(s)\Sigma U^{-1}(-s)$ be a unimodular matrix with $U(s)$ over $R[s]$ and Σ a signature matrix. Let $U(s)=Y(s)Z(s)$, where $Y(s)$ is unimodular and $Z(s)$ is the Hermite form of $U(s)$. Then $A(s)=Y(s)\bar{\Sigma}Y^{-1}(-s)$ for some signature matrix $\bar{\Sigma}$.*

Proof. Observe that

$$Y^{-1}(s)A(s)Y(-s)=Z(s)\Sigma Z^{-1}(-s)$$

is unimodular and polynomial because the left side has this property. For convenience, suppose that $\Sigma=I_{n_1}\dotplus(-I_{n_2})$, and partition $Z(s)$ conformably:

$$Z(s)=\begin{bmatrix} Z_{11}(s) & 0 \\ Z_{12}(s) & Z_{22}(s) \end{bmatrix}.$$

Then

$$Z(s)\Sigma Z^{-1}(-s)$$

$$=\left[\begin{array}{c|c} Z_{11}(s)Z_{11}^{-1}(-s) & 0 \\ \hline Z_{12}(s)Z_{11}^{-1}(-s)+Z_{22}(s)Z_{22}^{-1}(-s)Z_{12}(-s)Z_{11}^{-1}(-s) & -Z_{22}(s)Z_{22}^{-1}(-s) \end{array}\right]$$

Now the degree constraints and lower triangularity of $Z(s)$ ensure that

$$\lim_{s\to\infty} Z_{11}(s)Z_{11}^{-1}(-s)=\Sigma_1$$

for some signature matrix Σ_1. Because $Z_{11}(s)Z_{11}^{-1}(-s)$ is polynomial, we must have $Z_{11}(s)Z_{11}^{-1}(-s)=\Sigma_1$ for all s. Similarly, $Z_{22}(s)Z_{22}^{-1}(-s)=-\Sigma_2$ for all s, and $Z_{12}(s)Z_{11}^{-1}(-s)=0$ for all s. Thus

$$Z(s)\Sigma Z^{-1}(-s)=\begin{bmatrix}\Sigma_1 & 0\\ 0 & \Sigma_2\end{bmatrix}$$

and $A(s)=Y(s)[\Sigma_1 \dotplus \Sigma_2]Y^{-1}(-s)$, as required. ∎

This completes the proof of the Theorem. Embedded within the proof is a constructive procedure.

4. UNIQUENESS

In this section, we analyze the extent to which the decomposition is unique. The result is as follows.

THEOREM 2. *Let $A(s)$ be an $n\times n$ matrix such that $A(s)A(-s)=I$. Then in the decomposition*

$$A(s)=U(s)\Sigma U^{-1}(-s) \tag{1}$$

with $U(\cdot)$ unimodular, Σ is unique to within reordering, and if Σ is ordered to equal $I_{n_1}\dotplus(-I_{n_2})$, then $U(s)$ is unique to within right multiplication by a unimodular $V(s)$, arbitrary save that with

$$V(s)=\begin{bmatrix}V_{11}(s) & V_{12}(s)\\ V_{21}(s) & V_{22}(s)\end{bmatrix}$$

(where V_{11} has n_1 rows and columns), the submatrices V_{11} and V_{22} are even, while V_{12} and V_{21} are odd.

Proof. It is easily verified that if $U(s)$ in (1) is replaced by $\bar{U}(s)=U(s)V(s)$ with $V(s)$ as in the theorem statement, then $A(s)$ is unaltered.

Conversely, suppose that

$$U(s)\Sigma U^{-1}(-s)=\bar{U}(s)\Sigma\bar{U}^{-1}(-s)$$

with U and $\bar{U}$ unimodular. Set $V(s)=U^{-1}(s)\bar{U}(s)$. Then $V(s)$ is unimodular and

$$\Sigma V(-s)=V(s)\Sigma,$$

i.e.,

$$\begin{bmatrix} V_{11}(s) & -V_{12}(s) \\ V_{21}(s) & -V_{22}(s) \end{bmatrix}=\begin{bmatrix} V_{11}(-s) & V_{12}(-s) \\ -V_{21}(-s) & -V_{22}(-s) \end{bmatrix},$$

which proves the result. ∎

5. SIMPLE APPLICATION TO LINEAR SYSTEM THEORY

In linear system theory [3,4], we are often concerned with transfer function matrices of real rational functions of a variable s. Such matrices are often represented via a matrix fraction description, i.e., if $W(s)$ is real rational, we often have matrices $P(s),Q(s)$ over $R[s]$ with $P(s)$ nonsingular and with

$$W(s)=Q(s)P^{-1}(s). \tag{5}$$

Commonly, the pair $[P(s),Q(s)]$ is taken to be relatively right prime, i.e., any greatest common right divisor must be unimodular. This extends the notion of representing a rational function as a ratio of two coprime polynomials.

An important result of the theory [3,4] is that if QP^{-1} and SR^{-1} are two descriptions of the same W with $[P,Q]$ coprime and $[R,S]$ coprime, then there exists a unimodular $A(s)$ such that $QA=S$ and $PA=R$.

Now on occasions, $W(s)$ is even in s. For example if $W(s)$ is a rational power spectrum matrix of a vector random process $y(t)$, one has $W(s)=W'(-s)$; and if $y(t)$ is reversible—i.e., $E[y(t)y'(t+T)]=E[y(t)y'(t-T)]$—then $W(s)=W'(s)$, so that $W(s)=W(-s)$.

Given a matrix fraction description (5) with coprime $[P,Q]$ and evenness of $W(s)$, we have

$$Q(s)P^{-1}(s)=Q(-s)P^{-1}(-s),$$

and so there exists a unimodular $A(s)$ such that

$$Q(s)A(s)=Q(-s), \qquad P(s)A(s)=P(-s),$$

whence we see that $A(s)A(-s)=I$. By using the decomposition of (1) we can transform P,Q to reflect the evenness of $W(s)$ much more naturally. We set

$$\bar{P}(s)=P(s)U(s), \qquad \bar{Q}(s)=Q(s)U(s).$$

Then $W(s)=\bar{Q}(s)\bar{P}^{-1}(s)$, while also

$$\bar{P}(s)\Sigma=P(s)U(s)\Sigma=P(s)A(s)U(-s)=P(-s)U(-s)=\bar{P}(-s).$$

Similarly $\bar{Q}(s)\Sigma=Q(-s)$. Thus if $\Sigma=I_{n_1}\dotplus(-I_{n_2})$, we have

$$\bar{P}(s)=[\text{ Matrix of even polynomials } \vdots \text{ Matrix of odd polynomials }],$$

and similarly for $\bar{Q}(s)$. This is a matrix generalization of the fact that an even scalar rational function of s can be expressed as a ratio of two coprime polynomials, either both even or both odd.

REFERENCES

1 F. R. Gantmacher, *Matrix Theory*, Chelsea, New York, 1959.
2 C. C. Macduffee, *The Theory of Matrices*, Springer, Berlin, 1933.
3 H. H. Rosenbrock, *State-Space and Multivariable Theory*, Thomas Nelson and Sons, London, 1970.
4 W. A. Wolovich, *Linear Multivariable Systems*, Springer, New York, 1974.

Received 20 May 1977; revised 5 September 1977