PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 34, Number 2, August 1972

THE PSEUDOINVERSE OF AN r-CIRCULANT MATRIX

W. T. STALLINGS AND T. L. BOULLION

ABSTRACT. It is shown that the Moore-Penrose pseudoinverse C^+ of an r-circulant matrix C is always the conjugate transpose of an r-circulant matrix. In addition, necessary and sufficient conditions are given for C^+ to be an s-circulant matrix. Finally, a method for calculating C^+ is given.

I. **Introduction.** The Moore-Penrose pseudoinverse of a nonsingular $n\times n$ r-circulant matrix is an s-circulant matrix where $rs\equiv 1 \pmod n$. A similar statement is valid for some, but not all, singular r-circulant matrices. In this paper we show that the pseudoinverse of an r-circulant matrix is always the conjugate transpose of an r-circulant matrix, and use this result to describe the class of r-circulant matrices whose pseudoinverses are s-circulant matrices for some integer s.

II. **Background information.**

DEFINITION 1. An r-circulant matrix is an $n\times n$ complex matrix of the form

$$C = \begin{bmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-r} & a_{n-r+1} & \cdots & a_{n-r-1} \\ a_{n-2r} & a_{n-2r+1} & \cdots & a_{n-2r-1} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ a_r & a_{r+1} & \cdots & a_{r-1} \end{bmatrix}$$

where r is a nonnegative integer and each of the subscripts is understood to be reduced modulo n.

C^* and C^+ will denote respectively the conjugate transpose and Moore-Penrose pseudoinverse of the r-circulant C. (n, r) will denote the gcd of n and r.

DEFINITION 2. P will be the 1-circulant with first row $e_2^* = [0, 1, 0, \cdots, 0]$. Q_r will be the r-circulant with first row $e_1^* = [1, 0, \cdots, 0]$.

Received by the editors June 15, 1971 and, in revised form, October 4, 1971.
AMS 1970 *subject classifications*. Primary 15A09.
Key words and phrases. Pseudoinverse, r-circulant matrix.

PROPERTY 1 [3]. The Moore-Penrose pseudoinverse of a 1-circulant is a 1-circulant.

PROPERTY 2 [2]. The Moore-Penrose pseudoinverse of a nonsingular r-circulant in an s-circulant where s satisfies $rs\equiv 1 \pmod n$.

PROPERTY 3 [1]. C is an r-circulant if and only if $PC=CP^r$.

PROPERTY 4 [1]. If C and D are r- and s-circulants respectively, then CD is an rs-circulant.

PROPERTY 5 [1]. Let $\omega_1, \omega_2, \cdots, \omega_n$ be the nth roots of unity and let $R_i^*=(1/\sqrt{n})[1, \bar{\omega}_i, \bar{\omega}_i^2, \cdots, \bar{\omega}_i^{n-1}], i=1, 2, \cdots, n$. Then $\{R_i : i=1, 2, \cdots, n\}$ is an orthonormal set of eigenvectors for any $n\times n$ 1-circulant.

III. Main results.

THEOREM 1. *C is an r-circulant if and only if $(C^+)^*$ is an r-circulant.*

PROOF. By Property 3, $C=P^*CP^r$ where P is the unitary matrix described in Definition 2. Therefore

$$(C^+)^* = (P^{r*}C^+P)^* = P^*(C^+)^*P^r.$$

Using Property 3 again, we see that $(C^+)^*$ is an r-circulant. The uniqueness of C^+ gives the reverse implication.

We have said that if C is a singular r-circulant, C^+ may not be an s-circulant for any integer s. The 4×4 matrix Q_2 is an example. $Q_2^+=\frac{1}{2}Q_2^*$.

THEOREM 2. *If C is an $n\times n$ r_1-circulant then C^+ is an s_1-circulant if and only if there exists an integer r such that $(n, r)=1$ and C is also an r-circulant. In such a case there exists an integer s such that $rs\equiv 1 \pmod n$ and C^+ is also an s-circulant.*

In order to prove the "if" part of Theorem 2 we need two lemmas.

LEMMA 1. *The $n\times n$ matrix Q_r is unitary if and only if $(n, r)=1$.*

PROOF. From Definition 2 it is clear that

$$Q_r = \begin{bmatrix} e_1^* \\ e_{r+1}^* \\ \cdot \\ \cdot \\ \cdot \\ e_{(n-1)r+1}^* \end{bmatrix}.$$

Q_r will be singular if and only if there exist integers i and j satisfying $0\leqq i<j<n$ such that $ir\equiv jr \pmod n$; that is, if and only if there exists an

integer b such that

$$bn = ir - jr = (i-j)r. \tag{1}$$

Since $|i-j|<n$, (1) is valid if and only if $(n, r)>1$.

The following lemma is a result of Definitions 1 and 2.

LEMMA 2. *C is an r-circulant with first row* $[a_0, a_1, \cdots, a_{n-1}]$ *if and only if* $C=\sum_{i=0}^{n-1} a_i Q_r P^i$.

PROOF OF THEOREM 2 ("if" part only). If C is also an r-circulant where $(n, r)=1$, then $C=\sum_{i=0}^{n-1} a_i Q_r P^i = Q_r C_1$ where Q_r is unitary and C_1 is a 1-circulant with the same first row as C. By Properties 1, 2 and 4, $C^+ = C_1^+ Q_r^*$ is an s-circulant where $rs \equiv 1 \pmod{n}$.

Theorem 1 tells us that if we replace "C^+" with "C^*" in Theorem 2 we have a statement which is equivalent to Theorem 2. Hence we can complete the proof of Theorem 2 by proving the "only if" part for C^*.

LEMMA 3. *If C is an r-circulant with first row* $[a_0, a_1, \cdots, a_{n-1}]$ *then C^* is an s-circulant if and only if* $a_{irs}=a_i$, $i=0, 1, \cdots, n-1$, *where the subscripts are understood to be reduced modulo n.*

PROOF. Referring to Definition 1, the first column of C^* can be written as both

$$\begin{bmatrix} \bar{a}_0 \\ \bar{a}_1 \\ \bar{a}_2 \\ \cdot \\ \cdot \\ \cdot \\ \bar{a}_{n-1} \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} \bar{a}_0 \\ \bar{a}_{rs} \\ \bar{a}_{2rs} \\ \cdot \\ \cdot \\ \cdot \\ \bar{a}_{(n-1)rs} \end{bmatrix}.$$

The lemma follows from equating like elements and observing that C^* is completely described by specifying r and the first column of C^*.

PROOF OF THEOREM 2 ("only if" part). Suppose C and C^* are $n_1 \times n_1$ r_1- and s_1-circulants, respectively, such that $(r_1, n_1)>1$ and $(s_1, n_1)>1$. If $r_1=0$ or $s_1=0$ every element of C must be the same and C is an r-circulant for any r such that $0 \leqq r < n$. If $r_1 \neq 0$, define $n_2 = n_1/(r_1 s_1, n_1)$ and $k_1 = n_1/n_2$. By Lemma 3, $a_i = a_{n_2+i} = a_{2n_2+i} = \cdots = a_{(k_1-1)n_2+i}$, $i=0, 1, \cdots, n_1-1$. Thus C must be a composite of k_1^2 identical $n_2 \times n_2$ matrices. Define r_2 to be the modulo n_2 residue of r_1. Each of the $n_2 \times n_2$ matrices is an r_2-circulant and C is an h-circulant for all $h \in \{r_2 + jn_2 : j=0, 1, 2, \cdots, k_1-1\} = H$. If $(r_2, n_2)=1$ the collection $\{r_2 + jn_2 : j=0, \pm 1, \pm 2, \cdots\} = J$ contains infinitely many primes larger than n_1. Each element in J is congruent modulo n_1 to some element in H. But a prime larger than n_1 is congruent modulo n_1 to an element in the reduced residue system of n_1. Thus there exists an $r \in H$ such that $(r, n_1)=1$ and C is an r-circulant. If $r_2=0$ the situation is the same as when $r_1=0$.

If $(r_2, n_2)>1$, define s_2 to be the modulo n_2 residue of s_1 and repeat the above with n_2, n_3, r_2, s_2 and k_2. If $(r_3, n_3)>1$ continue to repeat the process until $(r_m, n_m)=1$ or $r_m=0$ for some m. The latter case yields the same situation as $r_1=0$ If $r_i \neq 0$ for any i we can guarantee that an m does exist such that $(r_m, n_m)=1$ since n_i divides n_{i-1}, $i=2, 3, \cdots, m$. Now C is an h-circulant for all $h \in \{r_m+jn_m : j=0, 1, \cdots, k_{m-1}-1\}=H_m$. As before, we can find an $r \in H_m$ such that $(r, n_1)=1$.

COROLLARY 1. *If C and D are $n\times n$ r-circulants then CD^* is a* 1-*circulant. If $(n, r)=1$ then C^*D is a* 1-*circulant.*

PROOF. CD^* is a 1-circulant since $CD^*=P^*CP^rP^{r*}D^*P=P^*CD^*P$.

We can now conclude that if C is an r-circulant, then CC^+ must be a 1-circulant, but C^+C may not be unless $(n, r)=1$. The 4×4 matrix Q_2 illustrates this point.

Calculation of C^+ is simple. Let R be the matrix whose columns are the R_i defined in Property 5. $R^*CC^*R=D$ is a diagonal matrix and $C^+= C^*(CC^*)^+=C^*RD^+R^*$. If there exists an r such that C is an r-circulant and $(n, r)=1$ the following formula is also valid and requires one less matrix multiplication:

$$C^+ = C_1^+Q_r^* = RD_1^+R^*Q_r^*,$$

where C_1 is defined as in the proof of Theorem 2 and $R^*C_1R=D_1$.

BIBLIOGRAPHY

1. C. M. Ablow and J. L. Brenner, *Roots and cannonical forms for circulant matrices*, Trans. Amer. Math. Soc. **107** (1963), 360–376. MR **27** #5775.

2. S. Charmonman and R. S. Julius, *Explicit inverses and condition numbers of certain circulants*, Math. Comp. **22** (1968), 428–430. MR **37** #2418.

3. G. H. Worm, *Explicit solutions for quadratic minimization problems*, Doctoral Dissertation, University of Tennessee, Knoxville, Tennessee, 1971.

4. I. Niven and H. S. Zuckerman, *An introduction to the theory of numbers*, Wiley, New York, 1960. MR **22** #5605.

DEPARTMENT OF MATHEMATICS, UNITED STATES AIR FORCE ACADEMY, COLORADO 80840

DEPARTMENT OF MATHEMATICS, TEXAS TECH UNIVERSITY, LUBBOCK, TEXAS 79409