Journal of Mathematical Sciences: Advances and Applications
Volume 12, Number 2, 2011, Pages 119-125

A DIHEDRAL APPROACH AT CIRCULANT MATRICES

JESÚS FERRER

Departamento de Análisis Matemático
Universidad de Valencia
Dr. Moliner, 50
46100 Burjasot
Valencia
Spain
e-mail: Jesus.Ferrer@uv.es

Abstract

We revisit some properties of circulant matrices regarding them as objects generated by the action of the dihedral group on complex vectors.

1. Introduction

As it is well known, a circulant matrix is a square matrix, whose successive rows are obtained by cyclic permutations of the first one. This type of matrices has been studied for quite a long time [1, 3, 4], and their properties have been used in the controllability of systems of differential equations [2], among other different applications. What we do here is to go over these properties looking at circulant matrices as objects generated by the action of the dihedral group over complex vectors.

2010 Mathematics Subject Classification: 32M25

Keywords and phrases: Complex vectors.

The author has been partially supported by MEC and FEDER Project MTM2008-03211.

Received November 4, 2011

To formalize this study, let $\sum_n$ represent the symmetric group of permutations of n objects, given a permutation $\sigma \in \sum_n$ and an n-dimensional complex vector $u = (a_1, a_2, \ldots, a_n) \in \mathbb{C}^n$, we define

$$\sigma u := (a_{\sigma_1}, a_{\sigma_2}, \ldots, a_{\sigma_n}).$$

It can be easily seen that this action of $\sum_n$ on $\mathbb{C}^n$ has the following properties:

If $\sigma \in \sum_n$, $u, v \in \mathbb{C}^n$, and $\lambda, \mu \in \mathbb{C}$,

(a) $\sigma(\lambda u + \mu v) = \lambda(\sigma u) + \mu(\sigma v)$.

(b) $\sigma u \bullet \sigma v = u \bullet v$, where $u \bullet v$ stands for the following matrix product:

If $u = (a_1, a_2, \ldots, a_n)$, $v = (b_1, b_2, \ldots, b_n)$,

$$u \bullet v = (a_1, a_2, \ldots, a_n) \cdot \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = \sum_{k=1}^{n} a_k b_k.$$

(c) $\sigma u \bullet v = u \bullet \sigma^{-1} v$.

Let Δ_n (the dihedral group) be the subgroup of $\sum_n$ generated by the n-cycle $\rho := (1, n, n-1, \ldots, 2)$ and the symmetry $\sigma := \prod_{j+k=n+1} (j, k)$. From a geometric perspective, ρ acts over an n-vertex regular polygon as a right-rotation of angle $\frac{2\pi}{n}$, while σ commutes the vertices 1 and n, 2 and $n-1$, and so on. Thus,

$$\Delta_n := \{\mathbf{1}, \rho, \rho^2, \ldots, \rho^{n-1}\} \cup \{\sigma, \rho\sigma, \rho^2\sigma, \ldots, \rho^{n-1}\sigma\},$$

and we list some equalities, which will be used later

$$\rho^{-1} = (1, 2, 3, \ldots, n); \quad (\rho^k\sigma)^{-1} = \rho^k\sigma, \quad \sigma\rho^k = \rho^{n-k}\sigma, \quad 0 \le k \le n-1.$$

Using this terminology, if $u = (a_1, a_2, \dots, a_n) \in \mathbb{C}^n$, the *circulant matrix* generated by u is

$$C_u := \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ a_n & a_1 & a_2 & \dots & a_{n-1} \\ a_{n-1} & a_n & a_1 & \dots & a_{n-2} \\ & & \dots & & \\ & & \dots & & \\ & & \dots & & \\ a_2 & a_3 & a_4 & \dots & a_1 \end{pmatrix},$$

and we shall represent C_u in either of these two ways.

By rows

$$C_u := \begin{pmatrix} u \\ \rho u \\ \rho^2 u \\ \vdots \\ \rho^{n-1} u \end{pmatrix}.$$

By columns

$$C_u := \left((\rho\sigma u)^t, (\rho^2\sigma u)^t, \dots, (\rho^{n-1}\sigma u)^t, (\sigma u)^t\right),$$

where v^t stands for the column obtained by transposing the row v.

Given $u = (a_1, a_2, \dots, a_n)$, $v = (b_1, b_2, \dots, b_n) \in \mathbb{C}^n$, and $\lambda, \mu \in \mathbb{C}$, the following properties are straightforward:

(1) $C_{\lambda u + \mu v} = \lambda C_u + \mu C_v$.

(2) $C_u \cdot C_v = C_w$, where $w = (u \bullet \rho\sigma v, u \bullet \rho^2 \sigma v, \dots, u \bullet \rho^{n-1} \sigma v, u \bullet \sigma v)$.

(3) $C_u \cdot C_v = C_v \cdot C_u$.

That is, the set of all circulant matrices forms a commutative subalgebra of the $(n \times n)$ complex matrices. To justify our notation, let us do some calculations

$$C_v \cdot C_u = \begin{pmatrix} v \\ \rho v \\ \rho^2 v \\ \vdots \\ \rho^{n-1} v \end{pmatrix} . \left((\rho\sigma u)^t, (\rho^2 \sigma u)^t, \ldots, (\rho^{n-1}\sigma u)^t, (\sigma u)^t \right)$$

$$= (\rho^{j-1} v \bullet \rho^k \sigma u)_{1 \leq j, k \leq n} = (\rho^k \sigma \rho^{j-1} v \bullet u)_{1 \leq j, k \leq n}$$

$$= (\rho^k \rho^{n-j+1} \sigma v \bullet u)_{1 \leq j, k \leq n} = (\rho^{k-j+1} \sigma v \bullet u)_{1 \leq j, k \leq n}$$

$$= (u \bullet \rho^{k-j+1} \sigma v)_{1 \leq j, k \leq n} = C_w = C_u \cdot C_v.$$

2. Diagonalization of Circulant Matrices

Making use of our dihedral notation, we show that every circulant matrix is diagonalizable over the field of complex numbers, whereas, in the real case, in order to be diagonalizable the circulant matrix needs to be symmetric.

Let $\omega := e^{2\pi i/n}$ be the complex n-th root of unity. For $u = (a_1, a_2, \ldots, a_n) \in \mathbb{C}^n$, we introduce the complex polynomial

$$P(z) := a_1 + a_2 z + a_3 z^2 + \ldots + a_n z^{n-1},$$

and the complex vectors

$$v_k = (1, \omega^{k-1}, \omega^{2(k-1)}, \ldots, \omega^{(n-1)(k-1)}), \quad 1 \leq k \leq n.$$

Noticing that

$$\rho^j u \bullet v_k = \omega^{j(k-1)} P(\omega^{k-1}), \quad 1 \leq j, k \leq n,$$

we have that

$$C_u \cdot v_k^t = P(\omega^{k-1}) v_k^t, \quad 1 \leq k \leq n.$$

Hence, since the vectors $v_1, v_2, \ldots, v_n$ are linearly independent, it follows that C_u is diagonalizable over $\mathbb{C}$, with the eigenvalues being

$$P(1),\ P(\omega),\ \ldots,\ P(\omega^{n-1}).$$

In the real case, the situation is different. Just notice that the (3×3) circulant matrix generated by the real vector (1, 2, 3) has $(\lambda - 6)(\lambda^2 + 3\lambda + 3)$ as characteristic polynomial and, since the second factor of this polynomial is irreducible in $\mathbb{R}$, the matrix $C_{(1,2,3)}$ is not diagonalizable over the reals.

The following proposition provides with a necessary and sufficient condition so that a real circulant matrix be diagonalizable over $\mathbb{R}$.

Proposition. *If* $u = (a_1, a_2, \ldots, a_n) \in \mathbb{R}^n$, *then the following assertions are equivalent*:

(i) $P(\omega),\ P(\omega^2),\ \ldots,\ P(\omega^{n-1})$ *are all real numbers.*

(ii) *The circulant matrix* C_u *is symmetric.*

(iii) C_u *is diagonalizable over* $\mathbb{R}$.

Proof. (i) $\Rightarrow$ (ii): For $k = 1, 2, \ldots, n-1$, from

$$P(\omega^k) = \overline{P(\omega^k)} = P(\overline{\omega}^k) = P(\omega^{k(n-1)}),$$

we obtain

$$(a_2 - a_n) + (a_3 - a_{n-1})\omega^k + \ldots + (a_n - a_2)\omega^{k(n-2)} = 0.$$

Hence, we have the following system of equalities:

$$\begin{cases} (a_2 - a_n) + (a_3 - a_{n-1})\omega + \ldots + (a_n - a_2)\omega^{n-2} = 0, \\ (a_2 - a_n) + (a_3 - a_{n-1})\omega^2 + \ldots + (a_n - a_2)\omega^{2(n-2)} = 0, \\ \ldots \\ \ldots \\ \ldots \\ (a_2 - a_n) + (a_3 - a_{n-1})\omega^{n-1} + \ldots + (a_n - a_2)\omega^{(n-1)(n-2)} = 0. \end{cases}$$

Since the Vandermonde $(n-1)$-determinant of the above system is nonzero, we deduce that

$$a_2 = a_n, \quad a_3 = a_{n-1}, \ldots .$$

Thus

$$\rho\sigma u = \rho(a_n, a_{n-1}, \ldots, a_1) = (a_1, a_n, \ldots, a_2) = (a_1, a_2, \ldots, a_n) = u.$$

Consequently, for $j = 1, 2, \ldots, n$,

$$\rho^j \sigma u = \rho^{j-1}\rho\sigma u = \rho^{j-1}u,$$

which, working by columns, leads us to

$$\begin{aligned} C_u^t &= \left(u^t, (\rho u)^t, \ldots, (\rho^{n-1}u)^t\right) \\ &= \left((\rho\sigma u)^t, (\rho^2\sigma u)^t, \ldots, (\rho^{n-1}\sigma u)^t, (\sigma u)^t\right) = C_u. \end{aligned}$$

Given that (ii) $\Rightarrow$ (iii) is evident, we show that (iii) $\Rightarrow$ (i).

If C_u is diagonalizable over $\mathbb{R}$, its characteristic polynomial admits n linear factors of real coefficients. From the complex case, we know that this polynomial is

$$(\lambda - P(1)) \cdot (\lambda - P(\omega)) \cdot \ldots \cdot (\lambda - P(\omega^{n-1})),$$

clearly then, the values

$$P(1), P(\omega), \ldots, P(\omega^{n-1})$$

must all be real numbers.

□

3. Inversion of Circulant Matrices

From the diagonalization study done above, it is easily seen that, for $u = (a_1, a_2, \ldots, a_n) \in \mathbb{C}^n$, the circulant matrix C_u is invertible, if and only if none of the values $P(1), P(\omega), \ldots, P(\omega^{n-1})$ is zero, i.e., when the polynomials $P(x)$ and $x^n - 1$ have no common divisors in $\mathbb{C}$.

Let C_u be an invertible circulant matrix. To see that the inverse matrix C_u^{-1} is also circulant, just recall that, if $e_1, e_2, \ldots, e_n$ denote the unit vectors of $\mathbb{C}^n$, then

$$\{C_{e_1}, C_{e_2}, \ldots, C_{e_n}\}$$

is a cyclic multiplication group generated by C_{e_2} and it can be easily seen that, for a square matrix M, M is circulant, if and only if $M \cdot C_{e_2} = C_{e_2} \cdot M$. Therefore, since $C_{e_n} \cdot C_u = C_u \cdot C_{e_n}$, we have that

$$C_u^{-1} \cdot C_{e_2} = C_u^{-1} \cdot C_{e_n}^{-1} = C_{e_n}^{-1} \cdot C_u^{-1} = C_{e_2} \cdot C_u^{-1},$$

i.e., C_u^{-1} is also circulant. Hence, the invertible circulant matrices form a commutative multiplication group. To calculate C_u^{-1}, let V be the Vandermonde matrix obtained by arranging the before defined vectors v_k, $1 \leq k \leq n$, in columns. Then, since $C_u = V \cdot \operatorname{diag}(P(1), P(\omega), \ldots, P(\omega^{n-1})) \cdot V^{-1}$, we have

$$C_u^{-1} = V \cdot \operatorname{diag}\left(\frac{1}{P(1)}, \frac{1}{P(\omega)}, \ldots, \frac{1}{P(\omega^{n-1})}\right) \cdot V^{-1} = C_{u'},$$

with

$$u' = \frac{1}{n}\left(\sum_{k=0}^{n-1} \frac{1}{P(\omega^k)}, \sum_{k=0}^{n-1} \frac{1}{\omega^k P(\omega^k)}, \ldots, \sum_{k=0}^{n-1} \frac{1}{\omega^{(n-1)k} P(\omega^k)}\right).$$

References

[1] Philip J. Davis, Circulant Matrices, Wiley Interscience, New York, 1974.

[2] Teodoro Lara, Matrices circulants, Divulgaciones Matemáticas 9(1) (2001), 85-102.

[3] Thomas Muir, The theory of circulants in the historical development up to 1860, Proc. Royal Soc. Edinburgh 2 (1906), 390-398.

[4] Alan C. Wilde, Transformations leaving the determinant of circulant matrices invariant, Amer. Math. Monthly, 93(5) (1986), 356-361.

■