ON CIRCULANT MATRICES

DARYL GELLER, IRWIN KRA, SORIN POPESCU AND SANTIAGO SIMANCA

1. Introduction

Fix a positive integer $n \geq 2$, and let

$$v = (v_0,\ v_1, \ldots, v_{n-1})$$

be a row vector in $\mathbb{C}^n$. Define the *shift* operator $T : \mathbb{C}^n \to \mathbb{C}^n$ by

$$T(v_0,\ v_1, \ldots, v_{n-1}) = (v_{n-1},\ v_0, \ldots, v_{n-2})\,.$$

The *circulant matrix* associated to v is the $n \times n$ matrix whose rows are given by iterations of the shift operator acting on v, that is to say, the matrix whose k-th row is given by $T^{k-1}v$, $k = 1, \ldots, n$. Such a matrix will be denoted by

$$V = \mathrm{circ}\{v\} = \mathrm{circ}\{v_0, v_1, \ldots, v_{n-1}\}\,.$$

Special cases of this type of matrices (see Theorem 3) appeared in one of the authors' recent work [7] based on [3]. They seem to be prevalent in certain parts of mathematics (see, for example, [5]). For reference purposes, we point the reader to the elegant treatment given in [4, §5.2], and the monograph [1] devoted to the subject.

Our work was originally motivated by the need to derive a specific result (Theorem 3) to be applied in the investigation of theta constant identities. Recently, our Theorem 3 has also been applied, in [6], to the theory of optimization in the field of management and information sciences.

Many facts about these matrices can be proven using *only* basic linear algebra. This makes the area quite accessible to undergraduates looking for "research problems." Our note presents a general view of these type of matrices, and hopes to illustrates the latter point by including in it a number of problems that may be of interest to students.

In our presentation, we concentrate on the discussion of necessary and sufficient conditions for circulant matrices to be nonsingular. This single goal allows us to lay out a rich mathematical structure surrounding these matrices, though this is by no means, an exhaustive treatment of all the properties they have. We have tried to make the note accessible to a wide audience by supplying rather full details in most of the arguments. When faced with the possibility of presenting a short argument or a longer one that requires less prerequisites, we have chosen the latter approach. At times the shorter, more elegant, argument is outlined in a remark.

The paper is organized as follows. We begin in §2 by evaluating the determinant of a circulant matrix, and computing some of its invariants. In §3, we discuss the space of such matrices, and show that it has the structure of a finite dimensional commutative algebra. Symmetries of circulant matrices are discussed briefly in §4. All this material is well known. Not so readily found in the literature is the remaining material. In §5, we determine necessary and sufficient conditions for a circulant matrix to be nonsingular provided n is prime. The case of real matrices is discussed in §6. We end our note by establishing, in §7, a relationship between the determinant of a circulant matrix and the rational normal curve in complex projective space. This material is not as elementary as the rest of our note, but illustrates the fact that circulant matrices have a strong presence in various parts of modern (and classical) mathematics. The interested reader may find a simpler illustration of this fact in [8].

It is a pleasure for Irwin Kra to thank Yum-Tong Siu, with whom he had enlightening conversations during a recent visit to Vietnam. Siu brought to his attention another, more elementary, proof of formula (1), and helped generate interest in the further study of circulant matrices. He also thanks Paul Fuhrmann for bringing to his attention a number of references, and for the helpful criticism of an earlier draft of this manuscript.

2. The general case

Theorem 1. *Let $v = (v_0, v_1, \ldots, v_{n-1})$ be a vector in $\mathbb{C}^n$, and $V = \operatorname{circ}\{v\}$. If ϵ is a primitive n-th root of unity, then*

$$\det V = \det \begin{bmatrix} v_0 & v_1 & \cdots & v_{n-2} & v_{n-1} \\ v_{n-1} & v_0 & \cdots & v_{n-3} & v_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ v_2 & v_3 & \cdots & v_0 & v_1 \\ v_1 & v_2 & \cdots & v_{n-1} & v_0 \end{bmatrix} = \prod_{l=0}^{n-1} \left(\sum_{j=0}^{n-1} \epsilon^{jl} v_j \right). \tag{1}$$

Proof. We view the matrix $V = \operatorname{circ}\{v_0, v_2, \ldots, v_{n-1}\}$ as a self map (linear operator) of $\mathbb{C}^n$. For each integer l, $0 \le l \le n-1$, let $x_l \in \mathbb{C}^n$

be the transpose of the row vector $\frac{1}{\sqrt{n}}(1, \epsilon^l, \epsilon^{2l}, \dots, \epsilon^{(n-1)l})$ and[1]

$$\lambda_l = v_0 + \epsilon^l v_1 + \cdots + \epsilon^{(n-1)l} v_{n-1}.$$

A calculation shows that

$$\begin{bmatrix} v_0 & v_1 & \cdots & v_{n-2} & v_{n-1} \\ v_{n-1} & v_0 & \cdots & v_{n-3} & v_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ v_2 & v_3 & \cdots & v_0 & v_1 \\ v_1 & v_2 & \cdots & v_{n-1} & v_0 \end{bmatrix} \begin{bmatrix} 1 \\ \epsilon^l \\ \epsilon^{2l} \\ \vdots \\ \epsilon^{(n-1)l} \end{bmatrix} = \lambda_l \begin{bmatrix} 1 \\ \epsilon^l \\ \epsilon^{2l} \\ \vdots \\ \epsilon^{(n-1)l} \end{bmatrix}.$$

Thus λ_l is an eigenvalue of V with normalized eigenvector x_l. Since $\{x_0, x_1, \dots, x_{n-1}\}$ is a linearly independent set, we conclude that

$$\det V = \prod_{l=0}^{n-1} \lambda_l\,.$$

□

Problem 1. Investigate the connection of the above result to the spectral mapping theorem.

Corollary 1. *The characteristic polynomial of V is*

$$p_V(x) = \det(xI - V) = \prod_{l=0}^{n-1}(x - \lambda_l).$$

Corollary 2. *The nullity of V is the number of zero eigenvalues λ_l.*

Corollary 3. *We have $\sum_{l=0}^{n-1} \lambda_l = nv_0$.*

Proof. Since

$$\sum_{l=0}^{n-1} e^{il} = \begin{cases} n & \text{for } i = 0 \\ 0 & \text{for } i = 1, \dots, n-1 \end{cases},$$

we see that

$$\sum_{l=0}^{n-1} \lambda_l = \sum_{l=0}^{n-1}\sum_{i=0}^{n-1} e^{li} v_i = \sum_{i=0}^{n-1}\left(\sum_{l=0}^{n-1} e^{li}\right) v_i = nv_0.$$

□

[1] We reserve the symbols λ_l and x_l for this eigenvalue and eigenvector throughout the manuscript. We use the convention, unless otherwise specified, that all vectors are column matrices. However, we will often write them as row matrices without mentioning that we are considering the transpose of the column vector. This identification should not cause any confusion. In a sense, it was already used in defining the shift operator T. In line with this convention, matrices, when viewed as linear operators, multiply column vectors on the left.

Remark 1. The last corollary also follows from the identity $\sum_{l=0}^{n-1} \lambda_l = \operatorname{trace} V$.

3. The space of Circulant matrices

Definition 1. We define $\mathrm{Circ}(n)$ to be the set of all $n \times n$ complex circulant matrices.

We record a number of consequences of the last theorem.

Corollary 4. $\mathrm{Circ}(n)$ *is an* n*-dimensional commutative subalgebra of the algebra of* $n \times n$ *matrices with the usual matrix operations of addition and multiplication. Furthermore, transposes of circulant matrices and inverses of nonsingular circulant matrices are also circulant. All elements of* $\mathrm{Circ}(n)$ *are simultaneously diagonalized by the same unitary matrix.*

Proof. Let C be the $n \times n$ matrix that represents the linear transformation sending the l-th unit vector e_l (this is the vector $(0, ..., 0, 1, 0, ..., 0)$ with the 1 in the l-th slot) to x_l:

$$C := \frac{1}{\sqrt{n}} \begin{bmatrix} 1 & 1 & \cdots & 1 & 1 \\ 1 & \epsilon & \cdots & \epsilon^{n-2} & \epsilon^{n-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & \epsilon^{n-2} & \cdots & \epsilon^{(n-2)^2} & \epsilon^{(n-1)(n-2)} \\ 1 & \epsilon^{n-1} & \cdots & \epsilon^{(n-2)(n-1)} & \epsilon^{(n-1)^2} \end{bmatrix},$$

and let D_V be the diagonal matrix with diagonal entries λ_0, λ_1, ..., λ_{n-2}, λ_{n-1}, respectively. Then

$$C^{-1} V C = D_V \,.$$

The remaining conclusions of the corollary follow readily now. $\square$

If we let

$$W = \mathrm{circ}\{0, 1, 0, \ldots, 0\},$$

then it is seen easily that

$$\mathrm{circ}\{v_0, v_1, \ldots, v_{n-1}\} = \sum_{i=0}^{n-1} v_i W^i.$$

Remark 2. With respect to the standard basis of $\mathbb{C}^n$, the shift operator T is represented by the transpose of the matrix W; that is, by $\mathrm{circ}\{0, 0, \ldots, 0, 1\}$.

Corollary 5. *The map that sends* W *to the indeterminate* X *establishes an isomorphism of algebras between* $\mathrm{Circ}(n)$ *and* $\mathbb{C}[X]/(X^n - 1)$.

Definition 2. Given a circulant matrix $V = \mathrm{circ}\{v_0, v_1, \ldots, v_{n-1}\}$, we define its *representer* as the polynomial $P_V(X) = \sum_{i=0}^{n-1} v_i X^i$.

Corollary 6. *For* $l = 0, \ldots, n-1$, *we have that* $\lambda_l = P_V\left(e^{\frac{2\pi\imath}{n} l}\right)$.

Corollary 7. *Let* V *be a circulant matrix with representer* $P_V(X)$. *The following are equivalent:*

(a) *The matrix* V *is singular.*
(b) $P_V\left(e^{\frac{2\pi\imath}{n} l}\right) = 0$ *for some* $l \in \mathbb{Z}$.
(c) *The polynomials* $P_V(X)$ *and* $X^n - 1$ *are not relatively prime.*

Remark 3. The nullity of a circulant matrix V with representer $P_V(X)$ is the degree of the greatest common divisor of $P_V(X)$ and $X^n - 1$.

Remark 4. For each $n \times n$ circulant matrix V, we have two polynomials: its representer P_V of degree $\leq n-1$ and its characteristic polynomial p_V of degree n. We can describe these polynomials rather explicitly in terms of the eigenvalues λ_l of V.

The characteristic polynomial p_V is the unique monic polynomial of degree n that vanishes at λ_l, $l = 0, 1, \ldots, n-1$. The representer P_V is the unique polynomial of degree $\leq n-1$ whose value at $e^{\frac{2\pi\imath l}{n}}$ is λ_l for $l = 0, 1, \ldots, n-1$.

The roots of the characteristic polynomial of an arbitrary $n \times n$ matrix V (these are the eigenvalues of the matrix V) are obtained by solving a monic n-degree polynomial equation. However, in the case of circulant matrices, the roots of p_V are easily calculated using the *auxiliary companion* polynomial P_V. Thus if a given polynomial p is known to be the characteristic polynomial of a *known* circulant matrix V, its zeroes can be readily found. This remark is the basis of [5]. It is thus of considerable interest to determine which monic polynomials are characteristic polynomials of circulant matrices. Further, if we are given that $p = p_V$ for some circulant matrix V, can we determine V, or equivalently P_V, directly from p?

We can obviously recover V from its representer. If $\lambda = (\lambda_0, \ldots, \lambda_{n-1})$ is an ordered set of eigenvalues, then there is a unique circulant matrix $V = \mathrm{circ}\{v\} = \mathrm{circ}\{v_0, v_1, \ldots, v_{n-1}\}$ whose ordered eigenvalues are λ:

$$v = \sqrt{n} C^{-1} \lambda \,.$$

Thus there are at most $(n-1)!$ (see Corollary 3) circulant matrices V with characteristic polynomial p_V. In particular, every monic polynomial p is the characteristic polynomial of some circulant matrix V.

But the argument above avoids completely the issue of finding the roots of p, as the given construction of V from p started by assuming we had the roots of the polynomial. So the more difficult question is the construction of V (or equivalently, it representer P_V) in terms of the coefficients of the polynomial p.

Problem 2. Describe the finite set of circulant matrices with fixed characteristic polynomial.

Problem 3. Let $\mathcal{P}$ be the space of polynomials of degree $\leq n-1$. We have seen that $\mathcal{P}$ is canonically isomorphic to $\mathrm{Circ}(n)$ and thus, for each $p \in \mathcal{P}$, there exists a unique $V \in \mathrm{Circ}(n)$ such that $p = p_V$. Let $\mathcal{M}$ be the space of monic polynomials of degree n. We obtain a map $\lambda : \mathcal{P} \mapsto \mathcal{M}$ by sending p to p_V.

We know that λ is surjective. The last problem asked for a description of $\lambda^{-1}(p)$ for arbitrary $p \in \mathcal{M}$. We now want to study the induced differential map $d\lambda$.

We have shown that for $q \in \mathcal{M}$,

$$q(x) = \prod_{i=0}^{n-1}(x - \lambda_i) = x^n + \sum_{i=0}^{n-1} a_i x^i \,,$$

and if for $p \in \lambda^{-1}(q)$,

$$p(x) = \sum_{i=0}^{n-1} v_i x^i \,,$$

we must have

$$n v_0 = \sum_{i=0}^{n-1} \lambda_i = a_{n-1} \,.$$

We can represent an arbitrary $p \in \mathcal{P}$ by its coordinates $v \in \mathbb{C}^n$ as in Definition 2. We represent a point in $\mathcal{M}$ by its roots as in Corollary 1. In these coordinates, the differential of λ is given by

$$d\lambda = \left[\frac{\partial \lambda_l}{\partial v_j}\right] = \left[e^{\frac{2\pi \imath l j}{n}}\right] = \sqrt{n} C.$$

It is constant and invertible. Thus the map λ is always a local homeomorphism. But it is not globally injective.

Does λ have a splitting map σ? In other words, is there a map $\sigma : \mathcal{M} \mapsto \mathcal{P}$ such that $\lambda \circ \sigma$ is the identity?

Corollary 8. *If for some k, $|v_k| > \sum_{j \neq k} |v_j|$, then the circulant matrix $V = \mathrm{circ}\{v_0, \ldots, v_{n-1}\}$ is nonsingular.*

Proof. Let $P_V(X)$ be the representer of V. If $P_V\left(e^{\frac{2\pi\imath}{n}l}\right)=0$ for some $l\in\mathbb{Z}$, then for $\eta=e^{\frac{2\pi\imath}{n}l}$,

$$v_k\eta^k=-\sum_{j\neq k}v_j\eta^j.$$

In particular

$$|v_k|\leq\sum_{j\neq k}|v_j|,$$

which contradicts the hypothesis. □

Corollary 9. *Let $d|n$, $d\geq 1$, and assume that the vector v consists of $\frac{n}{d}$ identical blocks (that is, $v_{i+d}=v_i$ for all i, where indices are calculated modulo n). Then $\lambda_l=0$ whenever dl is not a multiple of n; hence V is singular and its nullity is $\geq n-d$.*

Proof. For all l,

$$\lambda_l=\sum_{i=0}^{n-1}\epsilon^{li}v_i=\sum_{j=0}^{\frac{n}{d}-1}\sum_{i=0}^{d-1}\epsilon^{ldj}\left(\epsilon^{li}v_i\right)=\frac{1-\epsilon^{nl}}{1-\epsilon^{dl}}\sum_{i=0}^{d-1}\epsilon^{li}v_i,$$

provided dl is not a multiple of n. In particular, $\lambda_l=0$ for $1\leq l<\frac{n}{d}$. In general there are $n-d$ integers l such that $0\leq l<n$ and dl is not a multiple of n. □

Remark 5. In this case

$$P_V(X)=\left(\sum_{i=0}^{d-1}v_iX^i\right)\left(\frac{X^n-1}{X^d-1}\right)$$

and the polynomial $\frac{X^n-1}{X^d-1}$ of degree $n-d$ divides both $P_V(X)$ and X^n-1 (see Corollary 7).

Corollary 10. *Let $d|n$, $d\geq 2$, and assume that the vector v consists of $\frac{n}{d}$ consecutive constant blocks of length d (that is, $v_{id+j}=v_{id}$ for $i=0,1,\dots\frac{n}{d}-1$ and $j=0,1,\dots,d-1$). Then $\lambda_l=0$ whenever $l\neq 0$ and $l\equiv 0\mod\frac{n}{d}$, hence V is singular and its nullity is $\geq d-1$.*

Proof. In this case

$$\lambda_l=\sum_{i=0}^{n-1}\epsilon^{li}v_i=\sum_{j=0}^{\frac{n}{d}-1}\epsilon^{ldj}v_{dj}\sum_{i=0}^{d-1}\epsilon^{li}=\frac{1-\epsilon^{ld}}{1-\epsilon^{l}}\sum_{j=0}^{\frac{n}{d}-1}\epsilon^{ldj}v_{dj},$$

provided $l>0$. In particular, $\lambda_l=0$ for all $l=\alpha\frac{n}{d}$, with $\alpha=1,2,\dots,d-1$. □

Remark 6. In this case

$$P_V(X) = \left(\sum_{i=0}^{\frac{n}{d}-1} v_i X^{id} \right) \left(\frac{X^d - 1}{X - 1} \right)$$

and the polynomial $\frac{X^d-1}{X-1}$ of degree $d-1$ divides both $P_V(X)$ and X^n-1 (see Corollary 7).

4. Symmetries of Circ(n)

It is easy to see that

$$\det \mathrm{circ}\{v_0, v_1, \ldots, v_{n-1}\}$$
$$= (-1)^{k(n-1)} \det \mathrm{circ}\{v_k, v_{k+1}, \ldots, v_{n-1}, v_0, \ldots, v_{k-1}\}\,.$$

We also have that

$$\det \mathrm{circ}\{v_0, v_1, \ldots, v_{n-1}\} = (-1)^{n-1} \det \mathrm{circ}\{v_{n-1}, v_{n-2}, \ldots, v_1, v_0\}\,.$$

However, there is no obvious general relation between $\det \mathrm{circ}\{v_0, v_1, \ldots, v_{n-1}\}$ and $\det \mathrm{circ}\{v_{\sigma(0)}, v_{\sigma(1)}, \ldots, v_{\sigma(n-1)}\}$ in the case where σ is an arbitrary permutation of n elements.

Given an invertible scalar a, we also have the relation

$$\det \mathrm{circ}\{v_0, v_1, \ldots, v_{n-1}\} = a^{-n} \det \mathrm{circ}\{av_0, av_1, \ldots, av_{n-1}\}\,.$$

Problem 4. Investigate the action of the permutation group on n letters on Circ(n).

5. The case of n prime

Theorem 2. *Let $n \in \mathbb{Z}_{>0}$ be a prime. Assume that V has entries in $\mathbb{Q}^n$. Then*

$$\det V = \det \begin{bmatrix} v_0 & v_1 & \cdots & v_{n-2} & v_{n-1} \\ v_{n-1} & v_0 & \cdots & v_{n-3} & v_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ v_2 & v_3 & \cdots & v_0 & v_1 \\ v_1 & v_2 & \cdots & v_{n-1} & v_0 \end{bmatrix} = 0$$

if and only if either $\lambda_0 = 0$ or all the v_i are equal.

Proof. If all the v_i's are equal, then $\lambda_l = 0$ for all $l > 0$. We already know that the vanishing of some λ_l implies that $\det V = 0$. Conversely assume that $\det V = 0$ and that $\lambda_0 \neq 0$. Then $\lambda_l = 0$ for some positive integer $l < n$.

Again we take $\epsilon = e^{2\pi i/n}$. By our formula for λ_l, we see that ϵ^l is a root of the polynomial

$$p(x) = \sum_{i=0}^{n-1} v_i x^i.$$

However, since n is prime, ϵ^l is a primitive n-th root of unity, so the minimal polynomial of ϵ^l over the rationals is the cyclotomic polynomial

$$q(x) = \sum_{i=0}^{n-1} x^i.$$

Therefore p is a constant multiple of q. Consequently all v_i are equal, as desired. □

6. Real points

Theorem 3. *If $\{v_j\}_{0\leq j\leq n-1}$ is a weakly monotone sequence (that is, a nondecreasing or nonincreasing sequence) of nonnegative or nonpositive real numbers, then the matrix $V = \mathrm{circ}\{v_0, v_1, ..., v_{n-1}\}$ is singular if and only if for some integer $d|n$, $d \geq 2$, the vector $v = (v_0, v_1, \dots, v_{n-1})$ consists of $\frac{n}{d}$ consecutive constant blocks of length d.*
In particular, if the sequence $\{v_j\}_{0\leq j\leq n-1}$ is strictly monotone and nonpositive or nonnegative, then V is non-singular.

Proof. If the matrix V were singular, then its representer $P_V(X) = \sum_{i=0}^{n-1} v_i X^i$ would vanish at an n-th root of unity, say ϵ. We can easily see that it is sufficient to prove the theorem in the case when $\{v_j\}_{0\leq j\leq n-1}$ is a nonincreasing sequence of nonnegative real numbers; all other cases reduce to this one, by replacing ϵ with $\frac{1}{\epsilon}$ or by appropriately changing the signs of all the v_i's (see also the symmetries discussed in §4). We may thus assume in the sequel that

$$v_0 \geq v_1 \geq \dots v_{n-1} \geq 0.$$

Now $P_V(\lambda) = 0$ means that

$$v_0 + v_1\epsilon + \cdots + v_{n-1}\epsilon^{n-1} = 0$$

and hence also

$$v_0\epsilon + v_1\epsilon^2 + \cdots + v_{n-1}\epsilon^n = 0,$$

which yields

$$v_0 - v_{n-1} = (v_0 - v_1)\epsilon + (v_1 - v_2)\epsilon^2 + \cdots + (v_{n-2} - v_{n-1})\epsilon^{n-1}. \tag{2}$$

Observe that if $z_1, \dots, z_m$ are complex numbers such that

$$\sum_{i=1}^{m} z_i = \left|\sum_{i=1}^{m} z_i\right| = \sum_{i=1}^{m} \mid z_i \mid, \tag{3}$$

then $z_i \geq 0$ for all $i = 1, \ldots, m$. Since $|\epsilon| = 1$, it follows from (2) that $z_k = (v_{k-1} - v_k)\epsilon^k$, $k = 1, \ldots, n-1$ satisfy (3), and thus for each k either $v_{k-1} = v_k$, or $\epsilon^k = 1$. The latter holds only if ϵ is actually a d-th root of unity, for some divisor $d \geq 2$ of n, while k is a multiple of d, and the conclusions of the theorem follow easily now.

Indeed, to be specific, choose the smallest positive integer d such that $\epsilon^d = 1$. Then $d \geq 2$, $d|n$ and $\epsilon^k = 1$ for $1 \leq k \leq n$ if and only if $k = d, 2d, \ldots$ or $n = \frac{n}{d}d$. It follows that $v_k = v_{k-1} = \ldots = v_{k-(d-1)}$. □

Remark 7. (a) With an argument similar to the one in the proof above, one can show that if the sequence $\{v_j\}_{j=0}^{n-1}$ is non-increasing and $v_{n-1} > 0$, then $P(X) = \sum_{i=0}^{n-1} v_i X^i$ is non-zero for any X on the unit complex disk $|X| < 1$. This result can be applied to show that if $P(X) = \sum_{i=0}^{n-1} v_i X^i$ is a polynomial whose coefficients v_i are positive, then its zeros λ all lie in the annulus $m \leq |\lambda| \leq M$, where

$$m = \min\left\{\frac{v_i}{v_{i+1}};\ i = 0, 1, \ldots, n-2\right\}$$

and

$$M = \max\left\{\frac{v_i}{v_{i+1}};\ i = 0, 1, \ldots, n-2\right\}.$$

(b) The circulant matrices formed from the vectors $(-3, -1, 0, 2, 2)$ and $(-4, -1, 0, 2, 3)$ show that certain parts of the hypothesis cannot be weakened.

(c) For a real circulant matrix, $\lambda_l = 0$ if and only if $\lambda_{n-l} = 0$.

Problem 5. Investigate generalizations of the last theorem to the complex case.

We end this section with the related

Problem 6. Let $\mathcal{V} = \mathbb{C}^n$ and let G be a finite group of order n that acts by permutations on the coordinates of $\mathbb{C}^n$; that is, for $v = (v_1, ..., v_n) \in \mathcal{V}$ and $g \in G$,

$$g(v_1, ..., v_n) = (v_{g(1)}, ..., v_{g(n)}).$$

Then the fixed point set

$$\mathcal{V}^G = \{v \in \mathcal{V}; g(v) = v \text{ for all } g \in G\}$$

is a nontrivial subspace of $\mathcal{V}$ since it contains the vector $(1, ..., 1)$. It is reasonable to conjecture that

$$\dim \mathcal{V}^G \,|G\,. \tag{4}$$

• Construct an example to show that the conjecture as it stands is false.

• Can one add some hypotheses concerning the action of G on $\mathcal{V}$ so that the divisibility property (4) holds?

• Let $V = \{y_1, y_2, ..., y_r\}$ be a finite collection of vectors in $\mathcal{V}$ and let $G(V)$ be the span of the vectors $\{g(y_i); g \in G, i = 1, 2, ..., r\}$. Can one compute the dimension of $G(V)$ in terms of invariants of the group G and collection V?

• In particular, if $r = 1$, viewing $y = y_1$ as a row vector and ordering the elements of G as $\{g_1, ..., g_n\}$, we form an $n \times n$ matrix M whose k-th row is $g_k(y)$. Under what conditions is M nonsingular?

7. Circulant matrices and rational normal curves

There is an alternative, more complicated but more geometric, proof of Theorem 1. We present it in this section, which also shows the usefulness of circulant matrices in algebraic geometry, and that one can also study other invariants, besides the determinant, of (generic) circulant matrices; for example, their lower order minors.

Let us begin by recalling that complex projective n-space $\mathbb{P}^n$ is the set of one-dimensional subspaces of $\mathbb{C}^{n+1}$. A point $p \in \mathbb{P}^n$ is usually written as a homogeneous vector $[z_0 : \ldots : z_n]$, by which is meant the complex line spanned by $(z_0, \ldots, z_n) \in \mathbb{C}^{n+1} \setminus \{0\}$.

A polynomial $f \in \mathbb{C}[z_0, \ldots, z_n]$ does not in general descend to a function on $\mathbb{P}^n$. However, if f is a homogeneous polynomial of degree d, we can perfectly talk about the zeroes of f in $\mathbb{P}^n$ because we have the relation $f(\lambda z_0, \ldots, \lambda z_n) = \lambda^d f(z_0, \ldots, z_n)$. The *rational normal curve* $C_d \subset \mathbb{P}^d$ of degree d is defined to be the image of the map $\mathbb{P}^1 \to \mathbb{P}^d$, given by

$$[z_0 : z_1] \mapsto [z_0^d : z_0^{d-1} z_1 : \ldots : z_0 z_1^{d-1} : z_1^d] = [Z_0 : \ldots : Z_d] .$$

This set is easily seen to be the common zero locus of the polynomials $p_{ij} = Z_i Z_j - Z_{i-1} Z_{j+1}$ for $1 \leq i \leq j \leq d-1$. The ideal of C_d, $I(C_d) := \{f \in \mathbb{C}[Z_0, \ldots, Z_n] \mid f \equiv 0 \text{ on } C_d\}$ is actually generated by this family of polynomials.

In general, an algebraic subset $X \subset \mathbb{P}^n$ is defined to be the zero locus of a collection of homogeneous polynomials, and its ideal $I(X)$ consists of the set of polynomials that vanish on X.

Let us now think of $\{v_0, \ldots, v_{n-1}, \ldots, v_{2n-2}\}$ as a set of $2n-1$ independent variables, and consider the matrix (beloved by invariant theorists) with constant antidiagonals given by

$$M := \begin{bmatrix} v_0 & v_1 & \cdots & v_{n-2} & v_{n-1} \\ v_1 & v_2 & \cdots & v_{n-1} & v_n \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ v_{n-2} & v_{n-1} & \cdots & v_{2n-4} & v_{2n-3} \\ v_{n-1} & v_n & \cdots & v_{2n-3} & v_{2n-2} \end{bmatrix}.$$

This matrix is called the (*generic*) $n \times n$ *catalecticant* matrix. By the above observations, the 2×2-minors of M define the ideal of the rational normal curve $C = C_{2n-2} \subset \mathbb{P}^{2n-2}$ of degree $2n-2$,

$$\mathbb{P}^1 \ni [z_0 : z_1] \mapsto [z_0^{2n-2} : z_0^{2n-3} z_1 : z_0^{2n-4} z_1^2 : \ldots : z_1^{2n-2}] \in \mathbb{P}^{2n-2}.$$

The other ideals of minors of M have geometric significance too. Since the sum of m matrices of rank one has rank at most m, it follows that for each $k \in \{2, \ldots, n\}$ the ideal I_k of $k \times k$-minors of M vanishes on the union of the $(k-1)$-secant $(k-2)$-planes to the rational normal curve $C \subset \mathbb{P}^{2n-2}$. Actually, it turns out that the ideal I_k of $k\times k$-minors of M defines the (reduced) locus of these $(k-1)$-secant $(k-2)$-planes to C (Raymond Wakerling, unpublished Ph.D. thesis, Berkeley 1939; see [2] for a modern complete proof).

Note that the restriction of the matrix M to the $(n-1)$-dimensional linear subspace $\Lambda \subset \mathbb{P}^{2n-2}$ defined by

$$\Lambda = \{v_n - v_0 = v_{n+1} - v_1 = \cdots = v_{2n-2} - v_{n-2} = 0\}$$

coincides up to row permutations with the (generic) circulant matrix

$$V = \mathrm{circ}\{v_0, v_1, \ldots, v_{n-1}\}.$$

(Here we say that a circulant matrix V is generic if $\{v_0, \ldots, v_{n-1}\}$ are considered independent variables.)

On the other hand the intersection $\Lambda \cap C$, consists of the n points whose coordinates $[z_0 : z_1] \in \mathbb{P}^1$ satisfy the equations

$$(z_0^{n-2}, z_0^{n-3} z_1, \ldots, z_1^{n-2}) \cdot (z_0^n - z_1^n) = 0,$$

or equivalently $z_0^n - z_1^n = 0$. If ϵ is as above a primitive n-th root of unity, these n points have coordinates in $\Lambda[v_0 : \ldots : v_{n-1}]$

$$p_i = [1 : \epsilon^i : \epsilon^{2i} : \cdots : \epsilon^{(n-1)i}], \qquad i \in \{0, \ldots, n-1\}.$$

It follows that the restriction of I_k to Λ vanishes on the union of $(k-2)$-planes

$$\bigcup_{i_1, i_2, \ldots, i_{k-1} \in \{0, \ldots, n-1\}} \mathrm{span}(p_{i_1}, p_{i_2}, \ldots, p_{i_{k-1}}).$$

In particular, the determinant of the generic circulant matrix V vanishes on the union of the n distinct hyperplanes

$$\bigcup_{i\in\{0,\dots,n-1\}} \operatorname{span}(p_0, p_1, \dots, \widehat{p_i}, \dots, p_{n-1}),$$

where (as usual) in the last union, the symbol $\widehat{p_i}$ denotes that p_i does not appear. But the union of the above n distinct hyperplanes is defined by a single polynomial of degree n (product of linear forms vanishing on each of the hyperplanes), while the determinant of the generic circulant matrix V is also a polynomial of degree n. Thus, by degree reasons these polynomials must agree up to a non-zero scalar, ans hence the hypersurface $\{\det V = 0\} \subset \Lambda$ must coincide with this union of hyperplanes. Since $\operatorname{span}(p_0, p_1, \dots, \widehat{p_i}, \dots, p_{n-1})$ is the zero-locus of

$$\lambda_{n-i} = v_0 + \epsilon^{-i} v_1 + \cdots + \epsilon^{-i(n-1)} v_{n-1},$$

we deduce that $\det(V)$ factors as in the statement of Theorem 1.

A similar but slightly more involved argument shows that for all $k \in \{2, \dots, n\}$, the ideal of $k \times k$-minors of the generic circulant matrix $V = \operatorname{circ}\{v_0, v_1, \dots, v_{n-1}\}$ defines the (reduced) union of $(k-2)$-planes

$$\bigcup_{i_1, i_2, \dots, i_{k-1} \in \{0,\dots,n-1\}} \operatorname{span}(p_{i_1}, p_{i_2}, \dots, p_{i_{k-1}})$$

(in contrast with case of the generic catalecticant matrix, where all ideals of minors are prime).

References

[1] P.J. Davis, *Circulant Matrices*, John Wiley and Sons, 1979.

[2] D. Eisenbud, *Linear Sections of Determinantal Varieties*, Amer. J. Math. **110** (1988), 541–575.

[3] H.M. Farkas and I. Kra, *Theta Constants, Riemann Surfaces and the Modular Group*, Graduate Studies in Mathematics, vol. 37, American Mathematical Society, 2001.

[4] P.A. Fuhrmann, *A Polynomial Approach to Linear Algebra*, Universitext, Springer, 1996.

[5] D. Kalman and J.E. White, *Polynomial equations and circulant matrrices*, Amer. Math. Monthly **108** (2001), 821–840.

[6] G.J. Koehler, *Those Pesky No Free Lunch Theorems for Optimization*, preprint 2004.

[7] I. Kra, *Product identities for θ-constants and θ-constant derivatives*, in preparation.

[8] H.R. Parks & D.C. Wills, *An Elementary Calculation of the Dihedral Angle of the Regular n-Simplex*, Amer. Math. Monthly **109** (2002), 756-758.

State University of New York at Stony Brook
Stony Brook, NY 11794