On Circulant Matrices

Irwin Kra and Santiago R. Simanca

Some mathematical topics—circulant matrices, in particular—are pure gems that cry out to be admired and studied with different techniques or perspectives in mind.

Our work on this subject was originally motivated by the apparent need of the first author to derive a specific result, in the spirit of Proposition 24, to be applied in his investigation of theta constant identities [9]. Although progress on that front eliminated the need for such a theorem, the search for it continued and was stimulated by enlightening conversations with Yum-Tong Siu during a visit to Vietnam. Upon the first author's return to the U.S., a visit by Paul Fuhrmann brought to his attention a vast literature on the subject, including the monograph [4]. Conversations in the Stony Brook mathematics common room attracted the attention of the second author and that of Sorin Popescu and Daryl Geller* to the subject and made it apparent that circulant matrices are worth studying in their own right, in part because of the rich literature on the subject connecting it to diverse parts of mathematics. These productive interchanges between the participants resulted in [5], the basis for this article. After that version of the paper lay dormant for a number of years, the authors' interest was rekindled by the casual discovery by S. Simanca that these matrices are connected with algebraic geometry over the mythical field of one element.

Circulant matrices are prevalent in many parts of mathematics (see, for example, [8]). We point the reader to the elegant treatment given in [4, §5.2] and to the monograph [1] devoted to the subject. These matrices appear naturally in areas of mathematics where the roots of unity play a role, and some of the reasons for this will unfurl in our presentation. However ubiquitous they are, 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 or mathematics teachers searching for topics of unique interest to present to their students.

We concentrate on the discussion of necessary and sufficient conditions for circulant matrices to be nonsingular and on various distinct representations they have, goals that allow us to lay out the rich mathematical structure that surrounds them. Our treatment, though, is by no means exhaustive. We expand on their connection to the algebraic geometry over a field with one element, to normal curves, and to Toeplitz's operators. The latter material illustrates the strong presence these matrices have in various parts of modern and classical mathematics. Additional connections to other mathematics may be found in [11].

The paper is organized as follows. In the section "Basic Properties" we introduce the basic definitions and present two models of the space of circulant matrices, including that as a finite-dimensional commutative algebra. Their determinant and eigenvalues, as well as some of

Irwin Kra is emeritus professor of mathematics at State University of New York at Stony Brook. His email address is irwin@math.sunysb.edu.

Santiago R. Simanca is a visiting senior professor of mathematics at the Laboratoire Jean Leray, Nantes, France. His email address is srsimanca@gmail.com.

* *Our colleague Daryl died on February 5, 2011. We dedicate this manuscript to his memory.*

DOI: http://dx.doi.org/10.1090/noti804

their other invariants, are computed in the section "Determinants and Eigenvalues". In the section "The Space of Circulant Matrices" we discuss further the space of such matrices and present their third model identifying them with the space of diagonal matrices. In the section "Roots of Polynomials" we discuss their use in the solvability of polynomial equations. All of this material is well known. Not so readily found in the literature is the remaining material, which is also less elementary. In the section "Singular Circulant Matrices" we determine necessary and sufficient conditions for classes of circulant matrices to be nonsingular. The geometry of the affine variety defined by these matrices is discussed in the section "The Geometry of Circ(n)", where we also speculate on some fascinating connections. In the section "The Rational Normal Curves Connection" we establish a relationship between the determinant of a circulant matrix and the rational normal curve in complex projective space and uncover their connection to Hankel matrices. Finally, in the section "Other Connections—Toeplitz Operators" we relate them to the much-studied Toeplitz operators and Toeplitz matrices as we outline their use in an elementary proof of Szegö's theorem.

It is a pleasure for the first author to thank Yum-Tong Siu for outlining another elementary proof of formula (3) and for generating his interest in this topic. He also thanks Paul Fuhrmann for bringing to his attention a number of references on the subject and for the helpful criticism of an earlier draft of this manuscript. It is with equal pleasure that the second author thanks A. Buium for many conversations about the subject of the field with one element and for the long list of related topics that he brought to his attention.

Basic Properties

We fix hereafter a positive integer $n \geq 2$. Our main actors are the n-dimensional complex vector space $\mathbb{C}^n$ and the ring of $n \times n$ complex matrices $\mathbb{M}_n$. We will be studying the multiplication Mv of matrices $M \in \mathbb{M}_n$ by vectors $v \in \mathbb{C}^n$. In this regard, we view v as a column vector. However, at times, it is useful mathematically and more convenient typographically to consider

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

as a row vector. We define a *shift* operator $T : \mathbb{C}^n \to \mathbb{C}^n$ by

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

We start with the basic and key definition.

Definition 1. The *circulant matrix* $V = \mathrm{circ}\{v\}$ *associated to* the vector $v \in \mathbb{C}^n$ is the $n \times n$ matrix whose rows are given by iterations of the shift operator acting on v; its k^{th} row is $T^{k-1}v$, $k = 1, \ldots, n$:

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

We denote by $\mathrm{Circ}(n) \subset \mathbb{M}_n$ the set of all $n \times n$ complex circulant matrices.

It is obvious that $\mathrm{Circ}(n)$ is an n-dimensional complex vector space (the matrix V is identified with its first row) under the usual operations of matrix addition and multiplication of matrices by scalars; hence our first model for circulant matrices is provided by the $\mathbb{C}$-linear isomorphism

$$\text{(FIRST MODEL)} \qquad \mathcal{I} : \mathrm{Circ}(n) \to \mathbb{C}^n,$$

where $\mathcal{I}$ sends a matrix to its first row. Matrices can, of course, be multiplied, and one can easily check that the product of two circulant matrices is again circulant and that for this set of matrices, multiplication is commutative. However, we will shortly see much more and conclude that we are dealing with a mathematical gem. Before that we record some basic facts about complex Euclidean space that we will use.

The ordered n-tuples of complex numbers can be viewed as the elements of the inner product space $\mathbb{C}^n$ with its Euclidean (L^2-norm) and *standard orthonormal basis*

$$e_i = (\delta_{i,0}, \ldots, \delta_{i,n-1}),\ i = 0, \ldots, n-1,$$

where $\delta_{i,j}$ is the *Kronecker delta* (= 1 for $i = j$ and 0 for $i \neq j$). We will denote this basis by $\mathbf{e}$ and remind the reader that in the usual representation $v = (v_0,\ v_1, \ldots, v_{n-1}) = \sum_{i=0}^{n-1} v_i e_i$, the v_i's are the components of v with respect to the basis $\mathbf{e}$.

To explore another basis, we fix once and for all a choice of a primitive nth root of unity

$$\epsilon = e^{\frac{2\pi\imath}{n}},$$

define for $l = 0, 1, \ldots, n-1$,

$$x_l = \frac{1}{\sqrt{n}}(1, \epsilon^l, \epsilon^{2l}, \ldots, \epsilon^{(n-1)l}) \in \mathbb{C}^n,$$

and introduce a special case of the *Vandermonde matrix*

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

It is well known and established by a calculation that

$$\det E = n^{-\frac{n}{2}} \prod_{0 \leq i < j \leq n-1} (\epsilon^j - \epsilon^i) \neq 0; \tag{1}$$

hence E is nonsingular. In fact, E is a most remarkable matrix: It is *unitary*, $E^{-1} = \overline{E}^t$, and it is *symmetric*, $E^t = E$, and hence $E^{-1} = \overline{E}$; and its columns and rows are the vectors $\{x_l\}$.

We view E as a self-map of $\mathbb{C}^n$ and conclude that $Ee_i = E(e_i) = x_i$. Since E is nonsingular, we see that the $\{x_l\}$ are another orthonormal basis for $\mathbb{C}^n$, to be denoted by $\mathbf{x}$. The $\mathbb{C}$-linear self-map of $\mathbb{C}^n$ defined by the matrix E depends, of course, on the bases for the domain and target; to show this dependence, the map should be denoted as $E_{\mathbf{e},\mathbf{e}}$. Observe that as linear maps, $E_{\mathbf{e},\mathbf{e}} = I_{\mathbf{e},\mathbf{x}}$, where I is the $n \times n$ identity matrix.

To return to circulant matrices, we let

$$W_i = \operatorname{circ}\{e_i\}\,,\ 0 \le i \le n-1.$$

It is obvious that we have a *standard representation* or *form* of circulant matrices:

$$\operatorname{circ}\{(v_0, v_1, \ldots, v_{n-1})\} = \sum_{i=0}^{n-1} v_i W_i.$$

It is less obvious, but follows by an easy calculation, that $W_i W_j = W_{i+j}$, where all the indices are interpreted mod n. Obviously $W_0 = I$, and letting $W = W_1$, we see that $W^i = W_i$.

Remark 2. With respect to the standard basis of $\mathbb{C}^n$, the shift operator T is represented by the transpose W^t of the matrix W. Note that $(W^i)^t = W^{n-i}$.

It is useful to introduce

Definition 3. The (*polynomial in the indeterminate X*) *representer* P_V of the circulant matrix $V = \operatorname{circ}\{(v_0, v_1, \ldots, v_{n-1})\}$ is

$$P_V(X) = \sum_{i=0}^{n-1} v_i X^i\,. \tag{2}$$

As usual, we let $\mathbb{C}[X]$ denote the ring of complex polynomials and for $f(X) \in \mathbb{C}[X]$, $(f(X))$, the principal ideal generated by this polynomial. We have established most of the following theorem (the remaining claims are easily verified).

Theorem 4. *$\operatorname{Circ}(n)$ is a commutative algebra that is generated (over $\mathbb{C}$) by the single matrix W. The map that sends W to the indeterminate X extends by linearity and multiplicativity to an isomorphism of $\mathbb{C}$-algebras*

(SECOND MODEL) $\mathcal{J} : \operatorname{Circ}(n) \to \mathbb{C}[X]/(X^n - 1)$.

The map that sends a circulant matrix V to its transpose V^t is an involution of $\operatorname{Circ}(n)$ and corresponds under $\mathcal{J}$ to the automorphism of $\mathbb{C}[X]/(X^n - 1)$ induced by $X \mapsto X^{n-1}$.

Proof. The only nontrivial observation is that multiplication of circulant matrices in standard form corresponds to the multiplication in $\mathbb{C}[X]/(X^n - 1)$. □

Remark 5. The algebra $\mathbb{C}[X]/(X^n - 1)$ can be identified with the space $\mathcal{P}_{n-1}$ of complex polynomials of degree $\le (n-1)$ with appropriate definition of multiplication of its elements. Under this identification, for $V \in \operatorname{Circ}(n)$,

$$\mathcal{J}(V) = P_V(X).$$

Determinants and Eigenvalues

The Basic Theorem

Many results about circulants follow from direct calculations; in particular, the next theorem.

Theorem 6. *If $v = (v_0, v_1, \ldots, v_{n-1}) \in \mathbb{C}^n$ and $V = \operatorname{circ}\{v\}$, then*

$$\det V = \prod_{l=0}^{n-1} \left(\sum_{j=0}^{n-1} \epsilon^{jl} v_j \right) = \prod_{l=0}^{n-1} P_V(\epsilon^l). \tag{3}$$

Proof. We view the matrix V as a self-map $V_{\mathbf{e},\mathbf{e}}$ of $\mathbb{C}^n$. For each integer l, $0 \le l \le n-1$, let*

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

A calculation shows that $Vx_l = \lambda_l x_l$. Thus λ_l is an eigenvalue of V with normalized eigenvector x_l. Since, by (1), $\{x_0, x_1, \ldots, x_{n-1}\}$ is a linearly independent set of vectors in $\mathbb{C}^n$, the diagonal matrix with the corresponding eigenvalues is conjugate to V, and we conclude that $\det V = \prod_{l=0}^{n-1} \lambda_l$. □

Corollary 7. *All circulant matrices have the same ordered set of orthonormal eigenvectors $\{x_l\}$.*

Corollary 8. *The characteristic polynomial p_V of V is given by*

$$p_V(X) = \det(XI - V) = \prod_{l=0}^{n-1} (X - \lambda_l) = X^n + \sum_{i=n-1}^{0} b_i X^i. \tag{4}$$

(Here we let the last equality define the b_i's as functions of the λ_l's. They are the elementary symmetric functions of the λ_l's.)

Corollary 9. *The nullity of $V \in \operatorname{Circ}(n)$ is the number of zero eigenvalues λ_l.*

We use similar symbols for the characteristic polynomial p_V of a circulant matrix V and its representer P_V. They exhibit, however, different relations to V.

If we let $\nu(V)$ denote the nullity of V, the last corollary can be restated as

For all $V \in \operatorname{Circ}(n)$, $\nu(V) = \deg \gcd(p_V(X), X^n)$.

Corollary 10. *Let V be a circulant matrix with representer P_V. The following are equivalent:*

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

*Throughout this paper the symbols λ_l and x_l are reserved for the eigenvalue and eigenvectors we introduce here.

Again, we have a reformulation of part of the last corollary as

For all $V \in \mathrm{Circ}(n)$, $\nu(V) = \deg \gcd(P_V(X), X^n - 1)$.

Remark 11. The shift operator T acts on $\mathrm{Circ}(n)$. If $V \to T \cdot V$ denotes this action, then the traces of $T^k \cdot V$, $k = 0, \ldots, n-1$, uniquely determine V. The representer P_V of a circulant matrix V uniquely determines and is uniquely determined by the matrix. Similarly, the characteristic polynomial and eigenvalues of a circulant matrix uniquely determine each other. From a given set of ordered eigenvalues, we recover the circulant matrix by the next theorem. However, a given set of distinct eigenvalues determines $n!$ circulant matrices.

Determinants of Circulant Matrices

It is easy to see that

$$\begin{aligned}&\det \mathrm{circ}\{(\nu_0, \nu_1, \ldots, \nu_{n-1})\}\\ &\quad = (-1)^{n-1} \det \mathrm{circ}\{(\nu_1, \nu_2, \ldots, \nu_{n-1}, \nu_0)\}\\ &\quad = (-1)^{n-1} \det \mathrm{circ}\{(\nu_{n-1}, \nu_{n-2}, \ldots, \nu_1, \nu_0)\},\end{aligned}$$

and iterations of these yield that $\det V = (-1)^{k(n-1)} \det T^k \cdot V$ for each integer $0 \le k < n$. However, there is no obvious general relation between

$$\det \mathrm{circ}\{(\nu_0, \nu_1, \ldots, \nu_{n-1})\}$$

and

$$\det \mathrm{circ}\{(\nu_{\sigma(0)}, \nu_{\sigma(1)}, \ldots, \nu_{\sigma(n-1)})\}$$

for $\sigma \in \mathcal{S}_n$, the permutation group on n letters. For example,

$$\det \mathrm{circ}\{(\nu_0, \nu_1, \nu_2)\} = \nu_0^3 + \nu_1^3 + \nu_2^3 - 3\nu_0\nu_1\nu_2, \tag{5}$$

a function that is invariant under the permutation group $\mathcal{S}_3$, while

$$\begin{aligned}&\det \mathrm{circ}\{(\nu_0, \nu_1, \nu_2, \nu_3)\}\\ &\quad = (\nu_0 + \nu_1 + \nu_2 + \nu_3)(\nu_0 - \nu_1 + \nu_2 - \nu_3)\\ &\qquad \times ((\nu_0 - \nu_2)^2 + (\nu_1 - \nu_3)^2),\end{aligned} \tag{6}$$

which, though admitting some symmetries, fails to be invariant under the action of the entire group $\mathcal{S}_4$; for instance, it is not invariant under the transposition that exchanges ν_0 and ν_1.

The action of $\mathbb{C}^\times$ on $\mathrm{Circ}(n)$ by dilations can be used to understand further the singular circulant matrices. For given $a \in \mathbb{C}^\times$, we have that

$$\begin{aligned}&\det \mathrm{circ}\{(a\nu_0, a\nu_1, \ldots, a\nu_{n-1})\}\\ &\qquad = a^n \det \mathrm{circ}\{(\nu_0, \nu_1, \ldots, \nu_{n-1})\},\end{aligned}$$

and we may cast these matrices as the projective variety in $\mathbb{P}^{n-1}(\mathbb{C})$ given by the locus of det on $\mathrm{Circ}(n)$. The decomposition of this variety into its irreducible components yields a geometric interpretation of the zeroes of various multiplicities of this function on $\mathrm{Circ}(n)$.

The Space of Circulant Matrices

To obtain our third model for $\mathrm{Circ}(n)$, we start by defining $\mathbb{D}_n$ to be the space of $n \times n$ diagonal matrices. This space is clearly linearly isomorphic to $\mathbb{C}^n$.

Theorem 12. *All elements of* $\mathrm{Circ}(n)$ *are simultaneously diagonalized by the unitary matrix* E*; that is, for* V *in* $\mathrm{Circ}(n)$,

$$E^{-1}VE = D_V \tag{7}$$

is a diagonal matrix and the resulting map

$$\mathcal{D} : \mathrm{Circ}(n) \to \mathbb{D}_n \qquad \text{(THIRD MODEL)}$$

is a $\mathbb{C}$*-algebra isomorphism.*

Proof. The $n \times n$ matrix E represents the linear automorphism of $\mathbb{C}^n$ that sends the unit vector e_l to the unit vector x_l. If V is a circulant matrix and D_V is the diagonal matrix with diagonal entries given by the ordered eigenvalues of V: $\lambda_0, \lambda_1, \ldots, \lambda_{n-2}, \lambda_{n-1}$, then (7) holds. The map $\mathcal{D}$ is onto, because for all $D \in \mathbb{D}_n$, EDE^{-1} is circulant. □

Corollary 13. *The inverse of an invertible element of* $\mathrm{Circ}(n)$ *also belongs to* $\mathrm{Circ}(n)$.

Proof. If V is a nonsingular circulant matrix, then D_V is invertible and $D_V^{-1} = D_{V^{-1}}$. □

Corollary 14. *The characteristic polynomial of* $V \in \mathrm{Circ}(n)$ *is given by*

$$p_V(X) = \det(XI - V) = \det(XI - D_V).$$

Remark 15. The last corollary encodes several facts that can be established by other methods:

- Let $p \in \mathcal{P}_{n-1}$. If $p(X) = \sum a_i X^i$ and $\lambda_l = p(\epsilon^l)$, then the elementary symmetric functions of the λ_l's belong to the ring generated (over $\mathbb{Z}$) by the a_i's.
- Given an ordered set $\{\lambda_l\}$, the unique polynomial p satisfying $\lambda_l = p(\epsilon^l)$ is $\det(XI - D_V)$.

Roots of Polynomials

Each $n \times n$ circulant matrix V has two polynomials naturally associated to it: its representer P_V and its characteristic polynomial p_V. These are both described 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 each λ_l. The representer P_V is the unique polynomial of degree $\le n-1$ whose value at ϵ^l is λ_l.

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 degree n polynomial equation. In the case of circulant matrices, the roots of p_V are easily calculated using the representer 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 [8] and of the section "Polynomials of Degree ≤ 4". Every monic polynomial p is the characteristic polynomial of some circulant matrix V, and so a very natural problem ensues: If we are given that $p = p_V$ for a collection of circulant matrices V, can we determine one such V or, equivalently its representer P_V directly from p? If so, then the n roots of p are the values of P_V at the n nth roots of unity.

The General Case

The vector space $\mathcal{P}_{n-1}$ of polynomials of degree $\leq n-1$ is canonically isomorphic to $\mathrm{Circ}(n)$ (both are canonically isomorphic as vector spaces to $\mathbb{C}^n$). Let $\mathcal{M}$ be the affine space of monic polynomials of degree n (again identifiable with $\mathbb{C}^n$). We define a map

$$\Lambda : \mathcal{P}_{n-1} \to \mathcal{M}$$

as follows. For each $p \in \mathcal{P}_{n-1}$, there exists a unique $V \in \mathrm{Circ}(n)$ such that $p = P_V$. Send p to p_V. The map Λ is holomorphic; in fact, it is algebraic. We have already remarked that it is generically $n!$ to 1. We define three subspaces:

(1) $\mathcal{P}^0_{n-1}$ consisting of those

$$\{p \in \mathcal{P}_{n-1} \text{ with } p(\epsilon^i) \neq p(\epsilon^j) \text{ for all integers } 0 \leq i < j \leq n-1\}.$$

(2) $\mathrm{Circ}^0(n)$ consisting of those

$$\{V \in \mathrm{Circ}(n) \text{ with distinct eigenvalues}\}.$$

(3) $\mathcal{M}^0$ consisting of those

$$\{p \in \mathcal{M} \text{ with distinct roots}\}.$$

Each of the subspaces defined is open and dense in its respective ambient spaces. It is quite obvious that

$$\Lambda : \mathcal{P}^0_{n-1} \to \mathcal{M}^0$$

is a complex analytic bijection. An explicit form for the inverse to this map would provide an algorithm for solving equations of all degrees.

Remark 16. We know that

$$\mathcal{P}^0_{n-1} \cong \mathrm{Circ}^0(n) \cong \mathcal{M}^0.$$

Each of these spaces is defined analytically. However, the last one has an alternate algebraic characterization. Let p' denote the derivative of p. The set $\mathcal{M}^0$ can be described as

$$\{p \in \mathcal{M} : \deg \gcd(p, p') = 0\}.$$

Thus, solving general equations can be reduced by an algebraic procedure to solving equations with distinct roots, for the calculation of p' is quite algebraic, and so is the calculation of $d = \gcd(p, p')$ via the division algorithm. The polynomial $\frac{p}{d}$ has no multiple roots.

The problem encountered above is of fundamental importance and quite difficult in general. We now turn our attention to the cases of low degree.

Polynomials of Degree ≤ 4

Circulant matrices provide a unified approach to solving equations of degree ≤ 4; we will illustrate this for degrees 3 and 4. As is quite common, we start with a definition.

Definition 17. Given a monic polynomial p of degree n, a circulant $n \times n$ matrix $V = \mathrm{circ}\{(v_0, \ldots, v_{n-1})\}$ is said to *adhere* to p if the characteristic polynomial p_V of V is equal to p.

We learned at a quite early age that to solve the equation

$$p(X) = X^n + \alpha_{n-1}X^{n-1} + \alpha_{n-2}X^{n-2} + \cdots + \alpha_1 X + \alpha_0 = 0,$$

we should use the change of variable $Y = X + \frac{1}{n}\alpha_{n-1}$, which eliminates the monomial of degree $n-1$ in p and leads to the equation

$$q(Y) = Y^n + \gamma_{n-2}Y^{n-2} + \cdots + \gamma_1 Y + \gamma_0 = 0$$

to be solved. If $V = \mathrm{circ}\{(v_0, v_1, \ldots, v_{n-1})\}$ adheres to p, then the traceless matrix $V - v_0 I$ adheres to q.

A reasonable program for solving polynomial equations p of degree n can thus consist of changing variables to reduce to an equation q with zero coefficient monomial of degree $n-1$ and then finding a traceless circulant matrix V that adheres to q. The eigenvalues of V are the roots of $p_V = q$ and can be readily computed using the representer P_V of V. In this program we seem to be replacing the difficult problem of solving a monic polynomial equation of degree n by the more difficult problem of solving $n-1$ nonlinear equations in $n-1$ variables. However, because of the symmetries present in the latter set of equations, they may be easier to handle.

Cubics. We illustrate how this works for cubics by finding a circulant matrix $V = \mathrm{circ}\{(0, a, b)\}$ of zero trace that adheres to

$$q(Y) = Y^3 + \alpha Y + \beta.$$

We need to find *any* traceless 3×3 circulant matrix V that adheres to q. Evaluating the representer $P_V(Y) = aY + bY^2$ at $y = e^{j\frac{2\pi i}{3}}$, $j = 0, 1, 2$, will then yield the roots of q.

By formula (5) for $\det \mathrm{circ}\{(0, a, b)\}$, we see that

$$p_V(Y) = \det(YI - V) = Y^3 - 3abY - (a^3 + b^3),$$

and so

$$\begin{aligned} 3ab &= -\alpha, \\ a^3 + b^3 &= -\beta. \end{aligned}$$

It then follows that

$$a = \left(\frac{-\beta \pm \sqrt{\beta^2 + \frac{4\alpha^3}{27}}}{2}\right)^{\frac{1}{3}}, \quad b = \left(\frac{-\beta \mp \sqrt{\beta^2 + \frac{4\alpha^3}{27}}}{2}\right)^{\frac{1}{3}}$$

(we are free to choose any consistent set of values since we need only one representer), and the roots of q are given by (the values of P_V at the three cube roots of unity)

$$\begin{aligned} r_1 &= a+b, \\ r_2 &= ae^{\frac{2\pi\imath}{3}} + be^{2\frac{2\pi\imath}{3}}, \\ r_3 &= ae^{2\frac{2\pi\imath}{3}} + be^{\frac{2\pi\imath}{3}}. \end{aligned}$$

Quartics. In order to find the roots of the polynomial

$$q(Y) = Y^4 + \beta Y^2 + \gamma Y + \delta,$$

we search for a $V = \operatorname{circ}\{(0,b,c,d)\}$ such that $p_V(Y) = \det(YI - V) = q(Y)$. By (6),

$$\begin{aligned} p_V(Y) = Y^4 &- (4bd + 2c^2)Y^2 - 4c(b^2+d^2)Y \\ &+ (c^4 - b^4 - d^4 - 4bc^2d + 2b^2d^2), \end{aligned}$$

and so

$$\begin{aligned} 4bd + 2c^2 &= -\beta, \\ 4c(b^2+d^2) &= -\gamma, \\ c^4 - b^4 - d^4 - 4bc^2d + 2b^2d^2 &= \delta, \end{aligned}$$

a system in the unknowns a, b, c.

It suffices to say that this system admits solutions. We leave the details of the argument to the reader. We encourage the reader to explore two sets of additional symmetries: the first consisting of solutions of the system with $c = 0$, and the second, solutions with $b = d$.

Singular Circulant Matrices

The eigenvalues of a circulant matrix tell us when it is singular. We develop a number of criteria for singularity relying on this basic fact.

Proposition 18. *If for some k, $|v_k| > \sum_{j\neq k} |v_j|$, then the circulant matrix $V = \operatorname{circ}\{(v_0, \ldots, v_{n-1})\}$ is nonsingular. The result is sharp in the sense that $>$ cannot be replaced by $\geq$.*

Proof. Let P_V be the representer of V. If $P_V(\epsilon^l) = 0$ for some $l \in \mathbb{Z}$, then for $\lambda = \epsilon^l$,

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

In particular,

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

which contradicts the hypothesis. □

Proposition 19. *Let $d \mid n$, $1 \leq d < n$, and assume that the vector $v \in \mathbb{C}^n$ consists of $\frac{n}{d}$ identical blocks (that is, $v_{i+d} = v_i$ for all i, where indices are calculated* mod n*). Then $\lambda_l = 0$ whenever dl is not a multiple of n, and $V = \operatorname{circ}\{v\}$ is singular of nullity $\geq n - d$.*

Proof. Compute for $0 \leq l < n$,

$$\begin{aligned} \lambda_l = \sum_{i=0}^{n-1} \epsilon^{li} v_i &= \sum_{j=0}^{\frac{n}{d}-1} \left(\sum_{i=0}^{d-1} \epsilon^{l(dj+i)} v_{dj+i} \right) \\ &= \sum_{j=0}^{\frac{n}{d}-1} \epsilon^{ldj} \sum_{i=0}^{d-1} \epsilon^{li} v_i \\ &= \frac{1-\epsilon^{nl}}{1-\epsilon^{dl}} \sum_{i=0}^{d-1} \epsilon^{li} v_i, \end{aligned}$$

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 $0 < l < n$ and dl is not a multiple of n. □

Remark 20. In this case,

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

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 10).

Proposition 21. *Let $d \mid n$, $2 \leq d < n$, and assume that the vector $v \in \mathbb{C}^n$ consists of $\frac{n}{d}$ consecutive constant blocks of length d (that is to say, $v_{id+j} = v_{id}$ for $i = 0, 1, \ldots, \frac{n}{d} - 1$ and $j = 0, 1, \ldots, d-1$). Then $\lambda_l = 0$ whenever $l \neq 0$ and $l \equiv 0 \mod \frac{n}{d}$, and V is singular of nullity $\geq d - 1$.*

Proof. In this case

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

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

Remark 22. In the above situation,

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

and the polynomial $\frac{X^d-1}{X-1}$ of degree $d - 1$ divides both $P_V(X)$ and $X^n - 1$ (see Corollary 10).

Proposition 23. *Let $n \in \mathbb{Z}_{>0}$ be a prime. If $V = \operatorname{circ}\{(v_0, \ldots, v_{n-1})\}$ has entries in $\mathbb{Q}$, then* $\det V = 0$ *if and only if either $\lambda_0 = \sum_{j=0}^{n-1} v_j = 0$ or all the v_j's are equal.*

Proof. If all the v_i's are equal, then all the eigenvalues λ_l of V, except possibly λ_0, are equal to zero. We already know that the vanishing of one 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 $l < n$. Consider the field extension $\mathbb{Q}[\epsilon]$ and the automorphism A of this field

induced by sending $\epsilon \mapsto \epsilon^2$ (A fixes $\mathbb{Q}$, of course). Since n is prime, A generates a cyclic group of automorphisms of $\mathbb{Q}[\epsilon]$ of order $n-1$ that acts transitively on the primitive nth roots of unity: $\{\epsilon, \epsilon^2, \ldots, \epsilon^{n-1}\}$. Hence $\lambda_l = 0$ implies that $\lambda_k = 0$ for all integers k with $1 \le k \le n-1$. It remains to show that all the ν_i's are equal. Consider the $(n-1) \times n$ matrix

$$\begin{bmatrix} 1 & \epsilon & \epsilon^2 & \cdots & \epsilon^{n-1} \\ 1 & \epsilon^2 & \epsilon^4 & \cdots & \epsilon^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \epsilon^{n-1} & \epsilon^{2(n-1)} & \cdots & \epsilon^{(n-1)^2} \end{bmatrix}$$

(essentially the matrix E in the section "Determinants and Eigenvalues" with the first row deleted). Since it has rank $n-1$, this matrix, when viewed as a linear map from $\mathbb{C}^n$ to $\mathbb{C}^{n-1}$, must have a one-dimensional kernel. This kernel is spanned by the vector $(1, 1, \ldots, 1)$. The conclusion follows. □

Proposition 24. *If $\{\nu_j\}_{0 \le j \le n-1}$ is a weakly monotone sequence (that is, a nondecreasing or nonincreasing sequence) of nonnegative or nonpositive real numbers, then the matrix $V = \operatorname{circ}\{(\nu_0, \nu_1, \ldots, \nu_{n-1})\}$ is singular if and only if for some integer $d \mid n$, $d \ge 2$, the vector $\nu = (\nu_0, \nu_1, \ldots, \nu_{n-1})$ consists of $\frac{n}{d}$ consecutive constant blocks of length d. In particular, if the sequence $\{\nu_j\}_{0 \le j \le n-1}$ is strictly monotone and nonpositive or nonnegative, then V is nonsingular.*

Proof. If the matrix V were singular, then its representer P_V would vanish at an nth root of unity, say λ. It is sufficient to prove the theorem in the case when $\{\nu_j\}_{0 \le j \le n-1}$ is a nonincreasing sequence of nonnegative real numbers; all other cases reduce to this one by replacing λ with $\frac{1}{\lambda}$ or by appropriately changing the signs of all the ν_i's (see also the symmetries discussed at the beginning of the section "Polynomials of Degree ≤ 4"). We may thus assume in the sequel that

$$\nu_0 \ge \nu_1 \ge \cdots \ge \nu_{n-1} \ge 0.$$

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

$$\nu_0 + \nu_1\lambda + \cdots + \nu_{n-1}\lambda^{n-1} = 0,$$

and hence also that

$$\nu_0\lambda + \nu_1\lambda^2 + \cdots + \nu_{n-1}\lambda^n = 0,$$

which yields

$$\begin{aligned} \nu_0 - \nu_{n-1} = (\nu_0 - \nu_1)\lambda + (\nu_1 - \nu_2)\lambda^2 \\ + \cdots + (\nu_{n-2} - \nu_{n-1})\lambda^{n-1}. \end{aligned} \tag{8}$$

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

$$\sum_{i=1}^{m} z_i = \left| \sum_{i=1}^{m} z_i \right| = \sum_{i=1}^{m} |\, z_i \,|, \tag{9}$$

then $z_i \in \mathbb{R}$ and $z_i \ge 0$ for all $i = 1, \ldots, m$. Since $|\lambda| = 1$, it follows from (8) that the $z_k = (\nu_{k-1} - \nu_k)\lambda^k$, $k = 1, \ldots, n-1$, satisfy (9), and thus for each k either $\nu_{k-1} = \nu_k$ or $\lambda^k = 1$. The latter holds only if λ is actually a dth root of unity, for some divisor $d \ge 2$ of n, while k is a multiple of d, and the conclusions of the theorem now follow easily, for we may choose the smallest positive integer d such that $\lambda^d = 1$. Then $d \ge 2$, $d \mid n$ and $\lambda^k = 1$ for $1 \le k \le n$ if and only if $k = d, 2d, \ldots$ or $n = \frac{n}{d}d$. It follows that $\nu_k = \nu_{k-1} = \cdots = \nu_{k-(d-1)}$. □

The next result deals with circulant matrices whose entries are $\pm$ the same nonzero complex number.

Proposition 25. *If $V = \operatorname{circ}\{(\nu_0, \ldots, \nu_{n-1})\} \in \operatorname{Circ}(n)$ has entries in $\{\pm 1\}$, and $0 < k = |\{j \mid \nu_j = 1\}| \le n - k$, then*

(a) *$\lambda_0 = 0$ if and only if $k = \frac{n}{2}$.*
(b) *For $0 < l < n$, $\lambda_l = 0$ if and only if*

$$\sum_{\{j \mid \nu_j = 1\}} e^{lj} = 0.$$

(c) *Assume that $\lambda_0 \ne 0$. V is nonsingular provided that k is not of the form $\sum m_i p_i$, where the p_i run over the distinct positive prime factors of n and the m_i are positive integers. In particular, V is nonsingular if k is less than the smallest positive prime dividing n.*

Proof. If $0 \le l \le n$, the formula for the eigenvalues of V in terms of the representer P_V yields that

$$\lambda_l = \sum_{\{j \mid \nu_j = 1\}} \epsilon^{lj} - \sum_{\{j \mid \nu_j = -1\}} \epsilon^{lj}.$$

This establishes part (a). We now observe that

$$\sum_{\{j \mid \nu_j = 1\}} \epsilon^{lj} + \sum_{\{j \mid \nu_j = -1\}} \epsilon^{lj} = \sum_{j=0}^{n-1} \epsilon^{lj} = \frac{1 - \epsilon^{ln}}{1 - \epsilon^l} = 0,$$

for $0 < l < n$. Thus part (b) follows. For part (c), we observe that for $0 < l < n$ we have that $\lambda_l \ne 0$ by (b) and the characterization of vanishing sums of n-roots of unity of weight k proven in [10]. □

We end this section (see also [15]) with the following.

Proposition 26. *If*

$$V = \operatorname{circ}\left\{\left(1, \binom{n}{1} \ldots \binom{n}{n-1}\right)\right\},$$

then the following hold:

(a) *$\lambda_l = (1 + \epsilon^l)^n - 1$.*
(b) *$\lambda_l = 0$ if and only if $\frac{l}{n} = \frac{1}{3}$ or $\frac{l}{n} = \frac{2}{3}$.*
(c) *V is singular if and only if $n \equiv 0 \bmod 6$, in which case the nullity of V is 2.*

Proof. By Theorem 6, we have that

$$\lambda_l = \sum_{j=0}^{n-1} \binom{n}{j} \epsilon^{lj},$$

and the binomial expansion yields (a). We obtain that $\lambda_l = 0$ if and only if $(1+\epsilon^l)^n = 1$, and so $|1+\epsilon^l| = 1$ if and only if $\cos\frac{2\pi l}{n} = -\frac{1}{2}$, a statement equivalent to the condition $\frac{l}{n} = \frac{1}{3}$ or $\frac{l}{n} = \frac{2}{3}$. This proves (b). Part (c) follows readily since the conditions making $\lambda_l = 0$ are equivalent to n being divisible by 2 and 3, respectively, and λ_l being zero exactly for the two values of l satisfying the condition in (b). □

The Geometry of Circ(n)

Let k be a positive integer. The *affine k-space* over $\mathbb{C}$ is $\mathbb{C}^k$, often denoted by $\mathbb{A}^k_{\mathbb{C}}$. The maximal ideals in the polynomial ring $\mathbb{C}[x_1,\dots,x_k]$ correspond to elements of $\mathbb{C}^k$, with $a = (a_1,\dots,a_k) \in \mathbb{C}^k$ corresponding to the ideal in $\mathbb{C}[x_1,\dots,x_k]$ given by the kernel of the evaluation homomorphism $p \mapsto p(a)$. An *affine variety* $\mathbb{V} \subset \mathbb{C}^k$ is an irreducible component of the zero locus of a collection of polynomials $p_1,\dots,p_l$ in $\mathbb{C}[x_1,\dots,x_k]$. The ideal $I_{\mathbb{V}} = (p_1,\dots,p_l) \subset \mathbb{C}[x_1,\dots,x_k]$ of functions vanishing on $\mathbb{V}$ is prime, and under the above identification the points of V are in one-to-one correspondence with the set of maximal ideals of the ring $\mathcal{O}(\mathbb{V}) = \mathbb{C}[x_1,\dots,x_k]/I_{\mathbb{V}}$, a ring without zero divisors. We say that $\mathbb{V}$ *is cut out by* $p_1,\dots,p_l$, *has ideal* $I_{\mathbb{V}}$, and *ring of global functions* $\mathcal{O}(\mathbb{V})$. Theorem 4 realizes Circ(n) as the ring of global functions of the variety given by the nth roots of unity in $\mathbb{C}$.

Complex projective k-space $\mathbb{P}^k = \mathbb{P}^k_{\mathbb{C}}$ is the set of one-dimensional subspaces of $\mathbb{C}^{k+1}$. A point $x \in \mathbb{P}^k$ is usually written as a homogeneous vector $[x_0 : \dots : x_k]$, by which is meant the complex line spanned by $(x_0,\dots,x_k) \in \mathbb{C}^{k+1} \setminus \{0\}$.

A nonconstant polynomial $f \in \mathbb{C}[x_0,\dots,x_k]$ does not descend to a function on $\mathbb{P}^k$. However, if f is a homogeneous polynomial of degree d, we can talk about the zeroes of f in $\mathbb{P}^k$ because we have the relation $f(\lambda x_0,\dots,\lambda x_k) = \lambda^d f(x_0,\dots,x_k)$, for all $\lambda \in \mathbb{C} \setminus \{0\}$. A *projective variety* $\mathbb{V} \subset \mathbb{P}^k$ is an irreducible component of the zero locus of a finite collection of homogeneous polynomials.

If we replace the role of $\mathbb{C}$ in the above discussion by an arbitrary field $\mathbb{F}$, we obtain the notions of k-dimensional affine space $\mathbb{A}^k_{\mathbb{F}}$ and k-dimensional projective space $\mathbb{P}^k_{\mathbb{F}}$ over $\mathbb{F}$, respectively. Polynomials in $\mathbb{F}[x_1,\dots,x_k]$ define affine varieties in $\mathbb{A}^k_{\mathbb{F}}$, while homogeneous polynomials define projective varieties in $\mathbb{P}^k_{\mathbb{F}}$. These spaces are usually studied for algebraically closed $\mathbb{F}$, but the definitions are valid for more general fields, and we work in this extended context. Let $\mathbb{V}$ be an affine or projective variety over $\mathbb{F}$, the zero locus of a set of polynomials in $\mathbb{F}[x_1,\dots,x_k]$. Given any field extension $\mathbb{E}$ of $\mathbb{F}$, we can talk about the locus of these polynomials in the affine or projective space over the extension field $\mathbb{E}$. These will define the $\mathbb{E}$-points of the variety $\mathbb{V}$, a set which we denote by $\mathbb{V}(\mathbb{E})$. This brings about some additional structure to the $\mathbb{F}$-varieties $\mathbb{V}$, which we can think of as a functor from the category of field extensions of $\mathbb{F}$ and their morphisms to a suitable category of sets and morphisms, with the functor mapping an extension $\mathbb{E}$ of $\mathbb{F}$ to the set $\mathbb{V}(\mathbb{E})$ of $\mathbb{E}$-points of the variety. Using *restrictions* when possible, we may also use this idea in the opposite direction and find the points of a variety with coordinates in a subring of $\mathbb{F}$ when the variety in question is defined by polynomials whose coefficients are elements of the subring. This idea applied to Circ(n) takes us to a rather interesting situation.

Given a variety over $\mathbb{C}$ cut out by polynomials with coefficients in $\mathbb{Z}$, we can use the natural inclusion $\mathbb{Z} \hookrightarrow \mathbb{C}$ to look at the $\mathbb{Z}$-points of the variety and the restricted ring of global functions. In the case of Circ(n), the restricted ring of global functions is $\mathbb{Z}[X]/(X^n-1)$, and, remarkably, the set of prime ideals, or spectrum, of this latter ring is related to a variety defined over a *field with one element*, a mythical object denoted in the literature by $\mathbb{F}_1$. We elaborate on this connection. It derives from analogies between regular combinatorial arguments and combinatorics over the finite field $\mathbb{F}_q$ with q elements (q a power of a prime).

The number of bases of the $\mathbb{F}_q$-vector space $\mathbb{F}_q^k$ is given by $q^{\frac{k(k-1)}{2}}(q-1)^k[k]_q!$, where $[k]_q = 1+q+q^2+\cdots+q^{k-1}$, and where the q-factorial is defined by $[k]_q! = [1]_q \cdot [2]_q \cdots [k]_q$. Similarly, the number of linearly independent j-element subsets is equal to $q^{\frac{j(j-1)}{2}}(q-1)^k[k]_q!/[k-j]_q!$, and for $j \le k$, the number of subspaces of $\mathbb{F}_q^k$ of dimension j is given by

$$\binom{k}{j}_q = \frac{[k]_q!}{[k-j]_q![j]_q},$$

an expression that makes perfect sense when $q = 1$, in which case we obtain the usual binomial. The idea of the mysterious one element field $\mathbb{F}_1$ emerges [12], and we see that the number of $\mathbb{F}_1$-points of projective space—that is to say, the number of 1-dimensional subspaces of $\mathbb{F}_1^n$—must be equal to n. Speculating on this basis, we are led to define a vector space over $\mathbb{F}_1$ simply as a set, a subspace simply as a subset, and the dimensions of these simply as the cardinality of the said sets.

Some relationships between properties of Circ(n) and that of algebraic geometry over $\mathbb{F}_1$ now follow. We think of the group of points of $\mathbb{SL}(n,\mathbb{F}_1)$ as the symmetric group $\mathcal{S}_n$ on n letters and that these n-letters are the $\mathbb{F}_1$-points of the projective space $\mathbb{P}^{n-1}_{\mathbb{F}_1}$. A "variety X over $\mathbb{F}_1$" should have as extension to the scalars $\mathbb{Z}$, a

scheme $X_{\mathbb{Z}}$ of finite type over $\mathbb{Z}$, and the points of X should be a finite subset of the set of points in $X_{\mathbb{Z}}$. Going further, in developing algebraic geometry over $\mathbb{F}_1$, some [13] propose replacing the notion played by an ordinary commutative ring by that of a commutative, associative, and unitary monoid M to obtain $\mathrm{Spec}\,(M \otimes_{\mathbb{F}_1} \mathbb{Z}) = \mathrm{Spec}\,\mathbb{Z}[M]$. In particular, they define the finite extension $\mathbb{F}_{1^n}$ of degree n as the monoid $\mathbb{Z}/n\mathbb{Z}$, and its spectrum after lifting it to $\mathbb{Z}$ becomes

$$\mathrm{Spec}\,(\mathbb{F}_{1^n} \otimes_{\mathbb{F}_1} \mathbb{Z}) = \mathrm{Spec}\,(\mathbb{Z}[X]/(X^n - 1))\,.$$

Thus, the algebra of circulant matrices with integer coefficients is the ring of global functions of the spectrum of the field extension $\mathbb{F}_{1^n}$ of degree n after lifting it to $\mathbb{Z}$.

The Rational Normal Curves Connection

Theorem 6 has an elaborate proof that is more geometric in nature and longer than the proof by calculation given above. We outline its details.

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

$$\begin{aligned}[z_0 : z_1] &\mapsto [z_0^d : z_0^{d-1}z_1 : \cdots : z_0 z_1^{d-1} : z_1^d] \\ &= [Z_0 : \cdots : Z_d]\,.\end{aligned}$$

It is the common zero locus of the polynomials $p_{ij} = Z_iZ_j - Z_{i-1}Z_{j+1}$ for $1 \le i \le j \le d-1$. The ideal of C_d, $I(C_d) = \{f \in \mathbb{C}[Z_0, \ldots, Z_d] \mid f \equiv 0 \text{ on } C_d\}$ is generated by this set of polynomials.

We view $\{\nu_0, \ldots, \nu_{n-1}, \ldots, \nu_{2n-2}\}$ as a set of $2n-1$ independent variables and consider the matrix with constant antidiagonals given by

$$M = \begin{bmatrix} \nu_0 & \nu_1 & \cdots & \nu_{n-2} & \nu_{n-1} \\ \nu_1 & \nu_2 & \cdots & \nu_{n-1} & \nu_n \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \nu_{n-2} & \nu_{n-1} & \cdots & \nu_{2n-4} & \nu_{2n-3} \\ \nu_{n-1} & \nu_n & \cdots & \nu_{2n-3} & \nu_{2n-2} \end{bmatrix}$$

as an $n \times n$ *catalecticant* or *Hankel* matrix. Its 2×2-minors define the ideal of the rational normal curve $C = C_{2n-2} \subset \mathbb{P}^{2n-2}$ of degree $2n-2$.

The other ideals of minors of M also have geometric significance. Since the sum of m matrices of rank one has rank at most m, the ideal I_k of $k \times k$-minors of M, $k \in \{2, \ldots, n\}$, vanishes on the union of the $(k-1)$-secant $(k-2)$-planes to the rational normal curve $C \subset \mathbb{P}^{2n-2}$. The ideal I_k defines the (reduced) locus of these $(k-1)$-secant $(k-2)$-planes to C [14] (see [2] for a modern proof).

The restriction of M to the $(n-1)$-dimensional linear subspace

$$\Lambda = \{\nu_n - \nu_0 = \nu_{n+1} - \nu_1 = \cdots = \nu_{2n-2} - \nu_{n-2} = 0\} \subset \mathbb{P}^{2n-2}$$

coincides, up to row permutations, with the arbitrary circulant matrix

$$V = \mathrm{circ}\{(\nu_0, \nu_1, \ldots, \nu_{n-1})\}.$$

The intersection $\Lambda \cap C$ is the image in $\mathbb{P}^{2n-2}$ of the 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, $z_0^n - z_1^n = 0$. The point $[1 : \epsilon^i] \in \mathbb{P}^1$ gets mapped to the point

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

and so the restriction of I_k to Λ vanishes on

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

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

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

where the symbol $\widehat{p_i}$ indicates that p_i does not appear. The union of these n hyperplanes in $\mathbb{P}^{2n-2}$ is a degree n subvariety of codimension 1, and thus any degree n polynomial vanishing on it must be its defining equation, up to a scalar factor (because for any hypersurface, its defining ideal is generated by one element and the degree of the hypersurface is the degree of this element). We deduce that $\det(V)$ factors as in the statement of Theorem 6.

Similarly, though the argument is slightly more involved, we can show also that for all $k \in \{2, \ldots, n\}$, the ideal of $k \times k$-minors of the generic circulant matrix V defines the (reduced) 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 contrast with the case of the generic catalecticant matrix, where all ideals of minors are prime).

Other Connections—Toeplitz Operators

We end by discussing briefly a relation between circulant and Toeplitz matrices. The interested reader may consult [6] for more information about the connection.

Let $\{t_{-n+1}, \ldots, t_0, \ldots, t_{n-1}\}$ be a collection of $2n-1$ complex numbers. An $n \times n$ matrix $T = [t_{kj}]$ is said to be *Toeplitz* if $t_{kj} = t_{k-j}$. Thus, a Toeplitz matrix T is a square matrix of the form

$$T = T_n = \begin{bmatrix} t_0 & t_{-1} & \cdots & t_{-(n-2)} & t_{-(n-1)} \\ t_1 & t_0 & \cdots & t_{-(n-3)} & t_{-(n-2)} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ t_{n-2} & t_{n-3} & \cdots & t_0 & t_{-1} \\ t_{n-1} & t_{n-2} & \cdots & t_1 & t_0 \end{bmatrix}.$$

These matrices have a rich theory, and they relate naturally to the circulant ones we study here. If we have $t_k = t_{-(n-k)} = t_{k-n}$, then as a special case

T_n is circulant. We use both classes of matrices in a proof of a celebrated spectral theorem to show the depth of their interconnection.

Let φ be a smooth real-valued function on the unit circle with Fourier coefficients $\hat{\varphi}_j = \int_0^{2\pi} e^{-\imath j\theta}\varphi(\theta)d\theta$, and consider the Toeplitz matrix $T_n(\varphi) = (\hat{\varphi}_{i-j})$, $0 \le i, j \le n-1$. The renowned Szegö theorem [7] asserts that if f is a continuous function on $\mathbb{C}$, then

$$\lim_{n\to\infty} \frac{1}{n} \sum_{\lambda\in \mathrm{spec} T_n(\varphi)} f(\lambda) = \frac{1}{2\pi}\int_{\mathbb{S}^1} f(\varphi(e^{i\theta}))d\theta. \tag{10}$$

We sketch a classical argument leading to its proof.

Given a double sequence $\{t_k\}_{k=-\infty}^{+\infty} \subset \mathbb{C}$ in l^1 (and hence also in l^2), let φ be the L^1-function whose Fourier coefficients are the t_j's. We form the sequence of Toeplitz matrices $\{T_n(\varphi) = T_n\}_{n=1}^{+\infty}$, where T_n is defined, as above, by $\{t_{-n+1}, \dots, t_{n-1}\}$, and denote by $\tau_l^{(n)}$, $l = 0, 1, \dots, n-1$ its eigenvalues. The T_n's are Hermitian if and only if φ is real-valued. We study the *asymptotic distribution*

$$\lim_{n\to+\infty} \frac{1}{n}\sum_{l=0}^{n-1} \tau_l^{(n)}, \tag{11}$$

the case of $f(x) = x$ in Szegö's identity (10).

We introduce the circulant matrix $V_n(\varphi) = \mathrm{circ}\{(v_0^{(n)}, \dots, v_{n-1}^{(n)})\}$, where

$$v_k^{(n)} = \frac{1}{n}\sum_{j=0}^{n-1} \varphi\left(\frac{2\pi j}{n}\right) e^{\frac{2\pi jk}{n}i}. \tag{12}$$

For fixed k, this is the truncated Riemann sum approximation to the integral yielding t_{-k}, and since $\varphi \in L^1$, we have $v_k^{(n)} \to t_{-k}$. By Theorem 6, the ordered eigenvalues of $V_n(\varphi)$ are $\lambda_l^{(n)} = \varphi\left(2\pi\frac{l}{n}\right)$, $l = 0, \dots, n-1$, and so, using Riemann sums to approximate the integral of the mth power of φ, $m \in \mathbb{N}$, we conclude that

$$\lim_{n\to\infty} \frac{1}{n}\sum_{l=0}^{n-1} (\lambda_l^{(n)})^m = \frac{1}{2\pi}\int_0^{1\pi} \varphi(\theta)^m d\theta\,. \tag{13}$$

This relates the average of φ to the asymptotic distributions of the eigenvalues of V_n. The special case of Szegö's theorem above is now within reach.

If we can prove that the two sequences of $n\times n$ matrices $\{T_n\}$ and $\{V_n\}$ are *asymptotically equivalent* in the sense that $\lim_{n\to+\infty} ||T_n - V_n|| = 0$, where $\|V\|$ is the Hilbert-Schmidt norm of the operator V, then their eigenvalues are asymptotically equivalent in the sense that

$$\lim_{n\to+\infty} \frac{1}{n}\sum_{l=0}^{n-1} (\tau_l^{(n)} - \lambda_l^{(n)}) = 0,$$

and so (11) equals (13) for $m = 1$. It is convenient to do this by introducing the auxiliary circulant matrix $V_n(\pi_n\varphi) = \mathrm{circ}\{(\tilde{v}_0^{(n)}, \dots, \tilde{v}_{n-1}^{(n)})\}$ of the truncated Fourier series $\pi_n\varphi = \sum_{j=-n+1}^{n+1} t_j e^{ij\theta}$, where $\tilde{v}_k^{(n)}$ is given by (12) with the role of φ played by $\pi_n\varphi$. The matrix $V_n(\pi_n\varphi)$ is also Toeplitz, and its Toeplitz's coefficients are determined solely by $\{t_{-n+1}, \dots, t_{n-1}\}$. The matrices $V_n(\varphi)$ and $V_n(\pi_n\varphi)$ are asymptotically equivalent, and a simple L^2-argument of Fourier series shows that the latter is asymptotically equivalent to $T_n(\varphi)$, and so also the former.

Arbitrary powers of T_n and V_n have asymptotically equivalent eigenvalues, and the general Szegö's theorem follows by applying Weierstrass's polynomial approximation to f.

It is of practical significance that $V_n(\pi_n\varphi)$ encodes finite-dimensional information of the Fourier expansion of φ and spectral information on the zeroth order pseudodifferential operator $\pi_n M_\varphi \pi_n$, where M_φ is the multiplication by φ operator.

References

[1] P. J. Davis, *Circulant Matrices*, AMS Chelsea Publishing, 1994.

[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. Geller, I. Kra, S. Popescu, and S. Simanca, *On circulant matrices*, preprint, 2002 (pdf at `http://www.math.sunysb.edu/~sorin/eprints/circulant.pdf`).

[6] R. M. Gray, *Toeplitz and Circulant Matrices: A Review (Foundations and Trends in Communications and Information Theory)*, NOW, 2005.

[7] U. Grenander and G. Szegö, *Toeplitz Forms and Their Applications*, University of California Press, 1958.

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

[9] I. Kra, *Product Identities for θ-Constants and θ-Constant Derivatives*, in preparation.

[10] T. Y. Lam and K. H. Leung, On vanishing sums for roots of unity, *J. Algebra* **224** (2000), 91–109. Also arXiv:math/9511209, November 1995.

[11] H. R. Parks and D. C. Wills, An elementary calculation of the dihedral angle of the regular n-simplex, *Amer. Math. Monthly* **109** (2002), 756–758.

[12] J. Tits, *Sur les Analogues Algébriques des Groupes Semi-Simples Complexes*, Colloque d'algèbre supérieure, Bruxelles, 1956, pp. 261–289, Centre Belge de Recherches Mathématiques, Louvain; Librairie Gauthier-Villars, 1957, Paris.

[13] B. Töen and M. Vaquié, *Au-dessus de* Spec$\mathbb{Z}$, arXiv:math/0509684, October 2007.

[14] R. Wakerling, *On the loci of the $(K+1)$-secant K-spaces of a curve in r-space*, Ph.D. thesis, Berkeley, 1939.

[15] E. W. Weisstein, *Circulant Matrix*, from MathWorld—A Wolfram Web Resource, `http://mathworld.wolfram.com/CirculantMatrix.html`.