# Polynomial Equations and Circulant Matrices

**Dan Kalman and James E. White**

**1. INTRODUCTION.** There is something fascinating about procedures for solving low degree polynomial equations. On one hand, we all know that while general solutions (using radicals) are impossible beyond the fourth degree, they have been found for quadratics, cubics, and quartics. On the other hand, the *standard* solutions for the the cubic and quartic are complicated, and the methods seem ad hoc. How is a person supposed to remember them? It just seems that there ought to be a simple, memorable, unified method for all equations through degree four.

Approaches to unification have been around almost as long as the solutions themselves. In 1545, Cardano published solutions to both the cubic and quartic, attributing the former to Tartaglia and the latter to Ferrari. After subsequent work failed to solve equations of higher degree, Lagrange undertook an analysis in 1770 to explain why the methods for cubics and quartics are successful. From that time right down to the present, efforts have persisted to illuminate the solutions of cubic and quartic equations; see [**21**]. In this paper we present a unified approach based on circulant matrices. The idea is to construct a circulant matrix with a specified characteristic polynomial. The roots of the polynomial thus become eigenvalues, which are trivially found for circulant matrices.

This circulant matrix approach provides a beautiful unity to the solutions of cubic and quartic equations, in a form that is easy to remember. It also reveals other interesting insights and connections between matrices and polynomials, as well as cameo roles for interpolation theory and the discrete Fourier transform. We begin with a brief review of circulants, and then show how circulants can be used to find the zeroes of low degree polynomials. Succeeding sections explore how the circulant method is related to other approaches, present additional applications of circulants in the study of polynomial roots, and discuss generalizations using other classes of matrices.

**2. CIRCULANT MATRICES.** An $n \times n$ circulant matrix is formed from any $n$-vector by cyclically permuting the entries. For example, starting with $[a \;\; b \;\; c]$ we can generate the $3 \times 3$ circulant matrix

$$C = \begin{bmatrix} a & b & c \\ c & a & b \\ b & c & a \end{bmatrix}. \tag{1}$$

Circulant matrices have constant values on each downward diagonal, that is, along the lines of entries parallel to the main diagonal.

Circulant matrices have many interesting properties, only a few of which are considered in this paper. Circulants also play a significant role in several applications. For general presentations on circulant matrices see [**1**, Section 13.2] and [**5**].

What concerns us most about circulant matrices is the simple computation of their eigenvalues and eigenvectors using $n$th roots of unity. Here and throughout, we consider only *right* eigenvectors, which would appear as columns in the usual matrix notation. As a typographical convenience, we use the *tuple* format $(a, b, c)$ within running text.

For the $3 \times 3$ matrix $C$ in (1), we need the cube roots of unity: $1$, $\omega = (-1 + i\sqrt{3})/2$, and $\omega^2 = \overline{\omega}$. The eigenvalues of $C$ are then $a + b + c$, $a + b\omega + c\omega^2$, and $a + b\overline{\omega} + c\overline{\omega}^2$, with corresponding eigenvectors $(1, 1, 1)$, $(1, \omega, \omega^2)$, and $(1, \overline{\omega}, \overline{\omega}^2)$. These assertions are easily verified by direct computation. The key observation is that for any cube root of unity $\nu \neq 1$, successive powers cycle repeatedly through $1$, $\nu$, $\nu^2$.

The results for $3 \times 3$ circulants generalize to higher dimensions ($n > 3$) in the obvious way. This can again be verified computationally, but there is a cleaner approach that gives better insight about what is really going on. To begin with, we define a distinguished circulant matrix $W$ with first row $(0, 1, 0, \ldots, 0)$. $W$, which is just the identity matrix with its top row moved to the bottom, has many interesting attributes. For one thing, $W^T = W^{-1}$, so $W$ is an *orthogonal* matrix. For a complex matrix $A$, it is customary to consider the conjugate transpose, also called the *Hermitian* transpose, $A^*$. $A$ is *Hermitian* if $A = A^*$; it is *unitary* if $A^{-1} = A^*$; it is *normal* if $AA^* = A^*A$. Clearly unitary matrices and Hermitian matrices are always normal. In particular, since $W$ is a real matrix, $W^* = W^T$, so $W$ is unitary, and hence normal. An important result from matrix theory is the characterization of normal matrices as matrices that are unitarily diagonalizable. That is, $A$ is normal if and only if there exists a unitary $U$ such that $U^*AU$ is diagonal. We proceed to construct such a diagonalization for $W$.

Observe that $W$ is a permutation matrix representing a cyclic permutation of order $n$. This shows that the minimal polynomial for $W$ is $p(t) = t^n - 1$, and hence that the eigenvalues of $W$ are the $n$th roots of unity. For each $n$th root of unity $\nu$ an associated eigenvector is given by $v(\nu) = (1, \nu, \nu^2, \ldots, \nu^{n-1})$.

For concreteness, we express the $n$th roots of unity as powers of $\omega = e^{2\pi i/n}$. That gives the eigenvalues of $W$ as $\omega^0, \omega^1, \ldots, \omega^{n-1}$ with associated eigenvectors $v(\omega^0), v(\omega^1), \ldots, v(\omega^{n-1})$. Arranging these as the columns of a matrix $Q$ and entering the corresponding eigenvalues $\omega^k$ in the diagonal matrix $D$ leads to the identity

$$WQ = QD. \tag{2}$$

Note that $Q^{-1} = Q^*/n$, and therefore $(1/\sqrt{n})Q$ is unitary. Consequently, (2) can also be written in the form

$$W = \left(\frac{1}{\sqrt{n}}Q\right) D \left(\frac{1}{\sqrt{n}}Q\right)^*, \tag{3}$$

which is a *unitary* diagonalization of $W$. Next we extend these results about eigenvalues and eigenvectors for $W$ to general circulant matrices.

To that end, consider the algebra generated by $W$, namely, the matrices expressible as polynomials $q(W) = a_0 + a_1 W + a_2 W^2 + \cdots + a_{n-1} W^{n-1}$. There is a general relationship linking the eigenvalues of a matrix $A$ to those of any polynomial $q(A)$. Indeed, if $Av = \lambda v$, then $q(A)v = q(\lambda)v$. Here, taking $A$ to be $W$, each $v(\nu)$ is an eigenvector of $q(W)$, with corresponding eigenvalue $q(\nu)$. But the matrices $q(W)$ are precisely the circulant matrices. That is, if $C$ is any $n \times n$ circulant matrix, use its first row $[a_0 \;\; a_1 \;\; a_2 \;\; \ldots \;\; a_{n-1}]$ to define a polynomial $q(t) = a_0 + a_1 t + a_2 t^2 + \cdots + a_{n-1} t^{n-1}$. Then $C = q(W)$, and for any $n$th root of unity $\nu$, $q(\nu)$ is an eigenvalue of $C$. Moreover, every circulant $C = q(W)$ is diagonalized by $Q$. Specifically,

$$q(W)Q = Qq(D),$$

with corresponding unitary diagonalization

$$q(W) = \left(\frac{1}{\sqrt{n}}Q\right) q(D) \left(\frac{1}{\sqrt{n}}Q\right)^*.$$

A few examples should make this idea clear. Consider the circulant matrix

$$C = \begin{bmatrix} 1 & 2 & 1 & 3 \\ 3 & 1 & 2 & 1 \\ 1 & 3 & 1 & 2 \\ 2 & 1 & 3 & 1 \end{bmatrix}.$$

Here, with $n = 4$, the $n$th roots of unity are $\pm 1$ and $\pm i$. Read the polynomial $q$ from the first row of $C$ :

$$q(t) = 1 + 2t + t^2 + 3t^3.$$

The eigenvalues of $C$ are now computed as $q(1) = 7$, $q(-1) = -3$, $q(i) = -i$, and $q(-i) = i$, with corresponding eigenvectors

$$\begin{aligned} v(1) &= (1, 1, 1, 1), \\ v(-1) &= (1, -1, 1, -1), \\ v(i) &= (1, i, -1, -i), \quad \text{and} \\ v(-i) &= (1, -i, -1, i). \end{aligned}$$

The characteristic polynomial of $C$ is $\det(tI - C) = p(t) = t^4 - 4t^3 - 20t^2 - 4t - 21$.

Another example, somewhat contrived for later consideration, is

$$C = \begin{bmatrix} 1 & \sqrt[3]{2} & \sqrt[3]{4} \\ \sqrt[3]{4} & 1 & \sqrt[3]{2} \\ \sqrt[3]{2} & \sqrt[3]{4} & 1 \end{bmatrix}.$$

This time,

$$q(t) = 1 + \sqrt[3]{2}t + \sqrt[3]{4}t^2,$$

and we use the cube roots of unity, $1$, $\omega = (-1 + i\sqrt{3})/2$, and $\overline{\omega}$. The eigenvalues of $C$ are

$$q(1) = 1 + \sqrt[3]{2} + \sqrt[3]{4}$$

and

$$q(\omega),\ q(\overline{\omega}) = \left[2 - \sqrt[3]{2} - \sqrt[3]{4} \pm i\sqrt{3}(\sqrt[3]{4} - \sqrt[3]{2})\right] \Big/ 2.$$

The characteristic polynomial of $C$ is $p(t) = t^3 - 3t^2 - 3t - 1$.

As these examples suggest, circulants provide a novel way of constructing polynomials with known roots. Of course, given a set of roots, $r_j$, we can multiply the factors $(t - r_j)$ together to determine the coefficients of the corresponding polynomial. Typically, solving a polynomial equation involves the inverse process: start with the coefficients and extract the roots. Circulants offer a third perspective: begin with a circulant matrix $C = q(W)$ and generate *both* the coefficients *and* the roots of a polynomial $p$. Here, the polynomial $p$ is the characteristic polynomial of $C$; the coefficients can be obtained from the identity $p(t) = \det(tI - C)$; the roots, i.e., the eigenvalues of $C$, can be found by applying $q$ to the $n$th roots of unity. This perspective leads to a method for solving general quadratic, cubic, and quartic equations.

**3. SOLVING POLYNOMIAL EQUATIONS USING CIRCULANT MATRICES.** To illustrate the main idea of this section, we consider the problem of finding exact expressions for the roots of

$$p(t) = t^3 - 3t^2 - 3t - 1.$$

Normally, one might try to factor this polynomial in some way, or look for rational roots. However, we know from the preceding example that this $p$ is the characteristic polynomial of a corresponding circulant matrix

$$C = \begin{bmatrix} 1 & \sqrt[3]{2} & \sqrt[3]{4} \\ \sqrt[3]{4} & 1 & \sqrt[3]{2} \\ \sqrt[3]{2} & \sqrt[3]{4} & 1 \end{bmatrix},$$

so the roots of $p$ are the eigenvalues of $C$. But these are obtained by inspection as $q(1), q(\omega), q(\overline{\omega})$, where $q(t) = 1 + \sqrt[3]{2}t + \sqrt[3]{4}t^2$ and $\omega$ is a complex cube root of unity.

More generally, given a polynomial $p$, we try to find a corresponding circulant $C$ having $p$ for its characteristic polynomial. The first row of $C$ then defines a different polynomial $q$, and the roots of $p$ are obtained by applying $q$ to the $n$th roots of unity.

**Quadratics.** Let's work through this process for a general quadratic polynomial,

$$p(t) = t^2 + \alpha t + \beta.$$

We also consider a general $2 \times 2$ circulant

$$C = \begin{bmatrix} a & b \\ b & a \end{bmatrix}.$$

The characteristic polynomial of $C$ is

$$\det \begin{bmatrix} x - a & -b \\ -b & x - a \end{bmatrix} = x^2 - 2ax + a^2 - b^2.$$

We must find $a$ and $b$ so that this characteristic polynomial equals $p$, so

$$-2a = \alpha$$
$$a^2 - b^2 = \beta.$$

Solving this system gives $a = -\alpha/2$ and $b = \pm\sqrt{\alpha^2/4 - \beta}$. To proceed, we require only one solution of the system, and for convenience define $b$ with the positive sign, so

$$C = \begin{bmatrix} -\alpha/2 & \sqrt{\alpha^2/4 - \beta} \\ \sqrt{\alpha^2/4 - \beta} & -\alpha/2 \end{bmatrix}$$

and

$$q(t) = \frac{-\alpha}{2} + t\sqrt{\frac{\alpha^2}{4} - \beta}.$$

The roots of the original quadratic are now found by applying $q$ to the two square roots of unity:

$$q(1) = \frac{-\alpha}{2} + \sqrt{\frac{\alpha^2}{4} - \beta}$$

$$q(-1) = \frac{-\alpha}{2} - \sqrt{\frac{\alpha^2}{4} - \beta}.$$

Observe that defining $b$ with the opposite sign produces the same roots of $p$, although the values of $q(1)$ and $q(-1)$ are exchanged.

**Cubics.** A parallel analysis works for cubic polynomials. The general cubic is

$$p(t) = t^3 + \alpha t^2 + \beta t + \gamma,$$

and the general $3 \times 3$ circulant is

$$C = \begin{bmatrix} a & b & c \\ c & a & b \\ b & c & a \end{bmatrix}.$$

We want to find $a$, $b$, and $c$ so that $p$ is the characteristic polynomial of $C$, given by

$$\det \begin{bmatrix} x-a & -b & -c \\ -c & x-a & -b \\ -b & -c & x-a \end{bmatrix} = (x-a)^3 - b^3 - c^3 - 3bc(x-a).$$

This expression virtually demands the change of variables, $y = x - a$. Observe that the resulting equation has no quadratic term in $y$. Here we see that the circulant development inspires in a very natural way a preliminary step in the traditional solution of the cubic—making a linear change of variables to eliminate the quadratic term.

The general result, for $p(x) = x^n + \alpha_{n-1}x^{n-1} + \cdots$, is that the substitution $y = x - \alpha_{n-1}/n$ eliminates the term of degree $n-1$. This is easily derived by simple algebra. In the context of circulant matrices we gain a new way to think about this result. Recall that $-\alpha_{n-1}$ equals the sum of the roots of $p$. If $p$ is the characteristic polynomial of a matrix $C$, then the sum of the roots is the sum of the eigenvalues, that is, the trace, of $C$. Accordingly, eliminating the degree $n-1$ term corresponds to making the trace vanish. Now for a circulant matrix, the main diagonal is constant, say given by $a$, so the trace is $na = -\alpha_{n-1}$. This gives us two conclusions. First, $a = -\alpha_{n-1}/n$, which determines one of the parameters of the desired circulant matrix (and the constant term of the polynomial $q$). Second, as in the cubic case, $y = x - a = x - \alpha_{n-1}/n$ is the transformation that eliminates the term of degree $n-1$.

Looked at slightly differently, these remarks show that a linear change of variables can always be performed to eliminate the degree $n-1$ term of a polynomial of degree $n$, and the circulant matrix for the modified polynomial has vanishing diagonal and trace; such a matrix is called a *traceless circulant*. In solving the cubic and quartic equations, we assume that such a transformation has already been made. In particular, we restate the cubic case as follows. The object is to obtain expressions for the roots of $p(x) = x^3 + \beta x + \gamma$ as the eigenvalues of a circulant matrix

$$C = \begin{bmatrix} 0 & b & c \\ c & 0 & b \\ b & c & 0 \end{bmatrix}.$$

The characteristic polynomial of $C$ is

$$\det \begin{bmatrix} x & -b & -c \\ -c & x & -b \\ -b & -c & x \end{bmatrix} = x^3 - b^3 - c^3 - 3bcx.$$

This equals $p$ if

$$\begin{aligned} b^3 + c^3 &= -\gamma \\ 3bc &= -\beta. \end{aligned} \tag{4}$$

To complete the solution of the original equation, we must solve this system for $b$ and $c$, and then apply $q(x) = bx + cx^2$ to the cube roots of unity. That is, for any $a$ and $b$ satisfying (4), we obtain the roots of $p$ as $q(1) = b + c$, $q(\omega) = b\omega + c\omega^2$, and $q(\overline{\omega}) = b\overline{\omega} + c\overline{\omega}^2$.

Thinking of the unknowns as $b^3$ and $c^3$ makes (4) quite tractable. Indeed, dividing the second equation by 3 and cubing, we get

$$\begin{aligned} b^3 + c^3 &= -\gamma \\ b^3c^3 &= -\frac{\beta^3}{27}. \end{aligned}$$

Observe that $b^3$ and $c^3$ are the roots of the quadratic equation $x^2 + \gamma x - \beta^3/27 = 0$, and so are given by

$$\frac{-\gamma \pm \sqrt{\gamma^2 + 4\beta^3/27}}{2}. \tag{5}$$

At this point, it is tempting to write

$$\begin{aligned} b &= \left[\frac{-\gamma + \sqrt{\gamma^2 + 4\beta^3/27}}{2}\right]^{1/3} \\ c &= \left[\frac{-\gamma - \sqrt{\gamma^2 + 4\beta^3/27}}{2}\right]^{1/3}. \end{aligned} \tag{6}$$

Indeed, that is perfectly valid when all of the operations involve only real numbers. In the larger domain of complex numbers there is some ambiguity associated with the extraction of square and cube roots. In this case, define $b$ by (6), using *any* of the possible values of the necessary square and cube roots, and then take $c = -\beta/(3b)$. That produces a solution to (4), and leads to the roots of $p$ as already explained. All choices for $b$ result in the same roots.

This is not, of course, a new form for the solution of the cubic. Indeed, other derivations introduce systems of equations that are identical or essentially identical to (4); see [**11**, p. 318], [**13**], and [**21**]. Even the original solution published by Cardano in 1545 uses essentially the same equations [**4**, pp. 235–237]. What distinguishes our ap-

proach is the path leading up to (4) and the role of the roots of unity. In addition, the circulant approach extends immediately to the quartic equation.

**Quartics.** To complete this part of the paper, we outline the circulant solution of the quartic equation. The starting point is a general quartic polynomial

$$p(x) = x^4 + \beta x^2 + \gamma x + \delta,$$

and to avoid a trivial case, we assume that not all of $\beta$, $\gamma$, and $\delta$ vanish. We seek a circulant matrix

$$C = \begin{bmatrix} 0 & b & c & d \\ d & 0 & b & c \\ c & d & 0 & b \\ b & c & d & 0 \end{bmatrix}$$

with characteristic polynomial equal to $p$. The characteristic polynomial of $C$ is

$$\det \begin{bmatrix} x & -b & -c & -d \\ -d & x & -b & -c \\ -c & -d & x & -b \\ -b & -c & -d & x \end{bmatrix} = x^4 - (4bd + 2c^2)x^2 - 4c(b^2 + d^2)x + c^4 - b^4 - d^4 - 4bdc^2 + 2b^2d^2.$$

Equating this with $p$ produces the system

$$\begin{aligned} 4bd + 2c^2 &= -\beta \\ 4c(b^2 + d^2) &= -\gamma \\ c^4 - b^4 - d^4 - 4bdc^2 + 2b^2d^2 &= \delta. \end{aligned} \tag{7}$$

Now notice that the first and second equations in this system determine $bd$ and $b^2 + d^2$ in terms of $c$. This inspires us to rewrite the third equation in the form

$$c^4 - (b^2 + d^2)^2 + 4(bd)^2 - 4bdc^2 = \delta$$

and hence to obtain an equation in $c$ alone:

$$c^4 - \frac{\gamma^2}{16c^2} + \frac{(\beta + 2c^2)^2}{4} + (2c^2 + \beta)c^2 = \delta.$$

This simplifies to

$$c^6 + \frac{\beta}{2}c^4 + \left(\frac{\beta^2}{16} - \frac{\delta}{4}\right)c^2 - \frac{\gamma^2}{64} = 0, \tag{8}$$

which is a cubic polynomial equation in $c^2$, and in principle is solvable by the methods already in hand. This leads to a nonzero value for $c$ (since $\beta$, $\gamma$, and $\delta$ are not all 0), and it is then straightforward to find corresponding values for $b$ and $d$ so that (7) is satisfied. In this way we construct the circulant matrix $C = bW + cW^2 + dW^3 = q(W)$, whose eigenvalues are the roots of $p$. They are computed by applying $q$ to the fourth roots of unity:

$$q(1) = b + c + d$$
$$q(-1) = -b + c - d$$
$$q(i) = -c + i(b - d)$$
$$q(-i) = -c - i(b - d).$$

This completes the solution of the quartic, and the circulant approach to solving low degree polynomial equations. Next we look at connections between circulants and other approaches to solving polynomial equations.

**4. OTHER METHODS AND RELATED WORK.** As mentioned in the introduction, attempts to unify solutions to quadratic, cubic, and quartic equations date at least to Lagrange. This work is relevant to the topic at hand, and so we review it briefly. Our sources for this discussion are [**7**, p. 479], [**14**, pp. 330–334], and [**16**, pp. 600–606].

Lagrange's analysis characterized the general solutions of the cubic and quartic cases in terms of permutations of the roots, laying a foundation for the independent demonstrations by Abel and Galois of the impossibility of solutions by radicals for general equations of fifth degree. However, Lagrange did not unify the algebraic derivation of the solutions of the cubic and quartic. Following the analysis of Viete, he solved the cubic equation $x^3 + \beta x + \gamma = 0$ by introducing the transformation $x = y - \beta/(3y)$, obtaining a quadratic equation in $y^3$. His solution to the quartic $x^4 + \beta x^2 + \gamma x + \delta = 0$, essentially the same as the original solution of Ferrari, is to add $2yx^2 + y^2$ to each side and then rearrange to obtain a perfect square on the left:

$$x^4 + 2yx^2 + y^2 = (2y - \beta)x^2 - \gamma x + y^2 - \delta.$$

Now $y$ can be determined so that the expression on the right becomes a perfect square, allowing the quartic equation to be solved. In both of these cases, some algebraic manipulation leads to an auxiliary equation that can be solved. But there is no obvious connection between the manipulations introduced in each case. Once you see what to do, it is easy to verify that it gives a solution. But it is difficult to motivate the initial steps.

In the last century several authors have discussed approaches to low degree polynomials; see [**8**], [**12**], [**17**], [**19**], [**20**], [**21**], and [**23**]. Most of these involve some sort of algebraic manipulation that seems unmotivated, but that can be seen to lead to a solution. Sah's development [**19**] is virtually identical to the circulant approach presented here, although he places little emphasis on the circulant matrices (which he calls *cyclic*) and follows a development that, to us at least, seems less memorable and clear. More typically, Ungar [**21**] presents a unified approach to quadratic, cubic, and quartic equations by assuming in each case a particular form of the roots. For the cubic case, this turns out to be equivalent to assuming that the roots are $q(1)$, $q(\omega)$, and $q(\omega^2)$ as in our solution of the cubic in Section 3. In the quartic case his equations for the roots are very similar to what appears in the circulant approach, but his expressions are all combinations of 1 and $-1$; the circulant approach produces combinations of $1, -1, i$, and $-i$. However, Ungar does not explain why any of his expressions were selected. Oglesby [**17**] concentrates exclusively on the cubic case, and follows a development essentially the same as Ungar's. In the final section of this paper, we take a closer look at the approaches of Ungar and Sah, and see that they inspire a more general understanding of the circulant approach.

Circulant matrices have alternate guises that appear in other branches of mathematics closely associated with polynomials. We have already indicated that the circulants form an algebra with generator $W$. Each element is expressed as a polynomial of de-

gree $n-1$ or less in $W$, and, to compute products, we use the fact that powers of $W$ can be reduced modulo $n$. Equivalently, the circulant matrices can be realized as the quotient of a polynomial algebra modulo the ideal generated by the minimal polynomial of the generator $W$, namely, $t^n - 1$. In symbols, let $F[t]$ be the polynomial algebra over a field $F$, and let $\langle t^n - 1\rangle$ be the ideal generated by $t^n - 1$. Then the circulant matrices over $F$ are isomorphic to $F[t]/\langle t^n - 1\rangle$.

At the same time, the circulants over $F$ can equally be recognized as the *group algebra* over $F$ of the cyclic group of order $n$. In this setting, we recognize that the powers of $W$ form a cyclic group, as well as a basis for the algebra of circulants. In the group algebra we multiply elements of the basis according to the group law, and extend multiplication to the full algebra linearly. That is completely consistent with the way the operations behave in the matrix algebra.

These alternate characterizations of the circulant matrices are highly suggestive. They come tantalizingly close to the machinery of field extensions and Galois groups so familiar in the analysis of roots of polynomials. However, we have not been able to find meaningful connections between the circulant approach and the standard theory, nor have we found evidence that something like the circulant approach has already been explored in one of these other guises.

**5. WHAT ELSE CAN CIRCULANTS REVEAL?** The circulant approach exploits the connections between matrix algebra and roots of polynomials. These connections not only guide us to solutions of low degree equations, they also cast a new light on other properties of polynomials. We have already seen one example of this—a new route to the familiar result about eliminating the term of degree $n-1$ in a polynomial of degree $n$. In this section we exhibit a few more examples of this phenomenon.

One very attractive result concerns characterizing real polynomials with all real roots. Specifically, the real polynomial $p$ has all real roots if and only if any corresponding circulant matrix $C = q(W)$ is Hermitian. The proof is very simple. If the corresponding circulant is Hermitian, it as all real eigenvalues, so $p$ has all real roots. Conversely, suppose $p$ has all real roots, and let $C$ be any circulant matrix having $p$ for its characteristic polynomial. Thus $C$ has all real eigenvalues. We have already seen that $C$ is diagonalizable, satisfying

$$C = ADA^*$$

with $A = Q/\sqrt{n}$. Now we are assuming that the diagonal matrix $D$ of eigenvalues is real. In particular, $D = D^*$. Therefore, $C^* = (ADA^*)^* = AD^*A^* = C$.

This argument shows that the circulant matrices that correspond to a particular polynomial are either all Hermitian, or none are. At the end of this section we use these results to derive conditions that characterize real cubic and quartic polynomials that have all real roots.

The Hermitian characterization of a circulant with all real eigenvalues is just a special case of a more general result for normal matrices. As is well known, a normal matrix $A$ is (a) Hermitian if and only if its eigenvalues are all real, (b) unitary if and only if its eigenvalues are all of modulus 1, and (c) skew-Hermitian ($A^* = -A$) if and only if its eigenvalues are all pure imaginary. As already observed, applying the first of these results in the context of circulant matrices characterizes real polynomials with all real roots. Similarly, one sees that a polynomial has all roots of unit modulus if and only if the corresponding circulant matrix is unitary, and has all roots pure imaginary if and only if the corresponding circulant matrix is skew-Hermitian. The latter observation can be used to characterize polynomials with all imaginary roots, but that

amounts to little more than rotating the real results a quarter turn in the complex plane. Indeed, a given polynomial $p$ of degree $n$ has all roots pure imaginary if and only if the polynomial $p(iz)/i^n$ has all roots real.

The significance of the unitary case is less clear. We have not found a simple characterization of unitary circulants that translates easily into conditions about the corresponding characteristic polynomial. Note also that the reduction to a traceless polynomial does not preserve roots of modulus 1, so this simplification cannot be applied to the case of unitary circulant matrices. However, there is a related result. For a given polynomial $p$ of degree $n$, translate to eliminate the term of degree $n-1$, and then construct a corresponding traceless circulant matrix $C$. Then $C$ is unitary if and only if the roots of $p$ all lie on a circle of radius 1 centered at the mean of the roots. This would be an interesting topic to explore further.

How far can the circulant approach to solving polynomial equations be pushed? We know that a general solution by radicals is not possible for equations beyond the quartic, but why does the circulant method fail?

Let us consider the general problem of solving a polynomial equation of degree $n$ using circulants. A natural first question is whether every monic polynomial $p$ (say with complex coefficients) can be realized as the characteristic polynomial of a circulant matrix $C$. The answer is yes. If $r_1, r_2, \ldots, r_n$ are the roots of $p$, and if $\nu_1, \nu_2, \ldots, \nu_n$ are the $n$th roots of unity, then there is a unique interpolating polynomial $q$ of degree $n-1$ that maps $\nu_k$ to $r_k$ for each $k$. So says the theory of polynomial interpolation. But that means the circulant matrix $C = q(W)$ has eigenvalues that are precisely the roots $r_k$. Therefore, the characteristic polynomial of $C$ is the same as the given polynomial $p$. Conversely, it is evident that if $C = q(W)$ is a circulant with characteristic polynomial $p$ then $q$ is an interpolating polynomial that maps the roots of unity to the $r_k$. This shows that the circulants associated with $p$ are given precisely by the interpolating polynomials mapping roots of unity to roots of $p$.

Of course, if the roots of $p$ were known, one might set out to construct an interpolating polynomial $q$ explicitly. For concreteness, let us again define $\omega = e^{2\pi i/n}$, so that the $n$th roots of unity can be expressed as $\omega^k$ for $0 \le k < n$. We seek a polynomial $q(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ satisfying $q(\omega^k) = r_{k+1}$ for $0 \le k < n$. This leads naturally to a linear system for the coefficients $a_j$, in the form

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(n-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \cdots & \omega^{(n-1)^2} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{n-1} \end{bmatrix} = \begin{bmatrix} r_1 \\ r_2 \\ r_3 \\ \vdots \\ r_n \end{bmatrix}. \tag{9}$$

The system matrix is $Q$, which has inverse $Q^*/n$. This shows that the interpolation problem is always solvable. Indeed, $Q$ is familiar in the signal processing world as the matrix representation (up to a normalization convention) of the discrete Fourier transform (DFT). In this setting we can draw a somewhat surprising conclusion: the generating row of the circulant matrix for a polynomial $p$ is the inverse DFT of the roots of $p$. We show later that this idea of a linear mapping from a set of parameters (here, the generating row of the circulant) to the roots can be generalized. Whether there is any further significance to the connection with the DFT is open to speculation.

Incidentally, the foregoing discussion also makes it clear that there is not a unique circulant matrix corresponding to a given polynomial. If we reorder the roots $r_j$, then

we obtain a different interpolating polynomial $q$. If the $r_j$ are distinct, then any two permutations produce distinct interpolating polynomials, accounting for $n!$ different circulants associated with $p$.

Knowing that a circulant must exist for any $p$ is not the same thing as knowing how to find one. It is an exercise in Galois theory to show that the $n$th roots of unity are always expressible in terms of radicals [**9**, Exercise 15, p. 507]. The circulant method expresses the roots of $p$ in terms of these roots of unity and the coefficients of $q$. Since there are polynomials with rational coefficients whose roots cannot be expressed in terms of radicals, we observe that the circulant matrix entries for a given polynomial may likewise not be expressible in terms of radicals. This shows that the circulant matrix approach cannot possibly succeed in the general case.

On the other hand, there are characterizations of polynomial equations that are solvable by radicals [**15**, Chapter 5]. It would be interesting to see whether, subject to these characterizations, the circulant approach might be successful. This question, which was also raised by Sah [**19**], apparently remains open.

**Criteria for Real Roots.** We conclude this section with a discussion of criteria for a cubic or quartic with real coefficients to have all real roots. We know that these polynomials are characterized by the condition that the corresponding circulant is Hermitian, and that in turn leads to conditions on the coefficients of the polynomial. A related question concerns polynomials with rational coefficients and rational roots. The special case in which all of the entries in the corresponding circulant are also rational has been discussed in [**2**]. Using the results presented there, it is possible to derive conditions under which the circulant approach can be carried out without ever introducing irrational quantities. Although a complete treatment would be too great a digression here, we can state the result for the cubic case: the coefficients, roots, and circulant matrix are all rational for $x^3 + \beta x + \gamma$ if and only if $27\gamma^2 + 4\beta^3 = 0$.

Let us proceed with the discussion of real roots. A polynomial with real coefficients has real roots if and only if any corresponding circulant is Hermitian. For the cubic $p(x) = x^3 + \beta x + \gamma$, the associated circulant

$$\begin{bmatrix} 0 & b & c \\ c & 0 & b \\ b & c & 0 \end{bmatrix}$$

is Hermitian precisely when $b$ and $c$ are complex conjugates, and hence when $b^3$ and $c^3$ are complex conjugates. Now (5) ensures that $27\gamma^2 + 4\beta^3 \leq 0$ is a necessary and sufficient condition for $b$ and $c$ to be conjugates. That is, $p$ has three real roots if and only if $27\gamma^2 + 4\beta^3 \leq 0$.

There is also a nice geometric interpretation of the locations of the roots when all are real. With $c = \overline{b}$, we have roots $q(1) = b + \overline{b}$, $q(\omega) = \omega b + \overline{\omega}\overline{b}$, and $q(\overline{\omega}) = \overline{\omega} b + \omega \overline{b}$. These are the real parts of three points equally spaced around a circle in the complex plane. Indeed, let $h = 2b$. Then the roots of the cubic are the real parts of $h$, $\omega h$, and $\overline{\omega} h$, respectively, and these are equally distributed around the circle $|z| = |h|$. So geometrically, once we identify the complex number $b$, we can find the roots as follows: double $b$; with the result as one vertex, construct an equilateral triangle centered at the origin; project the vertices onto the real axis. This construction is illustrated in Figure 1. Although this construction applies in the special case of a traceless cubic (no quadratic term), the general case is essentially the same, because the general cubic $p(x) = x^3 + \alpha x^2 + \beta x + \gamma$ can be transformed to a traceless cubic by translating the

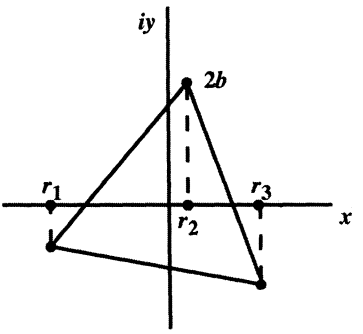


**Figure 1.** Vertices project to roots.

independent variable by an amount $\alpha/3$. The roots of the general cubic are still projections of the vertices of an equilateral triangle, but the center is at $-\alpha/3$, rather than at the origin. Interactive graphical computer explorations of these ideas are available on the internet: see [**24**] and [**25**].

For the quartic $p(x) = x^4 + \beta x^2 + \gamma x + \delta$, we assume as before that not all of the coefficients are zero. The circulant is

$$\begin{bmatrix} 0 & b & c & d \\ d & 0 & b & c \\ c & d & 0 & b \\ b & c & d & 0 \end{bmatrix},$$

which is Hermitian just when $d = \overline{b}$ and $c$ is real. Now any solution to (7) produces a circulant with characteristic polynomial $p$. Following the earlier analysis, such a solution can be constructed using any $c$ satisfying (8). Therefore, in order for all roots of $p$ to be real, and hence for all corresponding circulants to be Hermitian, it is necessary that all roots of (8) be real. Since (8) is cubic in $c^2$, the necessary condition reduces to this: the cubic

$$x^3 + \frac{\beta}{2}x^2 + \left(\frac{\beta^2}{16} - \frac{\delta}{4}\right)x - \frac{\gamma^2}{64} = 0 \tag{10}$$

must have all real, nonnegative roots. Conversely, if (10) has all real, nonnegative roots, then $p$ has all real roots. This can be proved using circulant matrices by constructing a solution of (7) for which the corresponding circulant is Hermitian. We defer this part of the proof for now. A much simpler argument involving a different class of matrices is given in a later section. The final conclusion, in any case, is the following characterization: the roots of $p$ are all real if and only if (10) has all real nonnegative roots.

As before, we have reached a known conclusion from an unexpected direction. There are direct methods in the theory of equations for deriving equivalent characterizations. Van der Waerden [**22**, pp. 190–192] handles the quartic case as follows. If the four roots of $p(x) = x^4 + \beta x^2 + \gamma x + \delta$ are $x_1, x_2, x_3, x_4$, then consider the cubic polynomial $r$ (called the *resolvant cubic*) with roots $(x_1 + x_2)(x_3 + x_4)$, $(x_1 + x_3)(x_2 + x_4)$, and $(x_1 + x_4)(x_2 + x_3)$. Using the elementary symmetric functions and the fact that $x_1 + x_2 + x_3 + x_4 = 0$, he shows that $r(x) = x^3 - 2\beta x^2 + (\beta^2 - 4\delta)x + \gamma^2$. Now the roots $x_k$ are all real if and only if the roots of $r$ are all real and nonpositive. This is

equivalent to the earlier result because $-r(-4x)/64$ equals the cubic in (10). But the two derivations have very different flavors. We return to the discussion of real roots in the next section. In that discussion (10) is referred to as the *resolvant cubic*.

We have shown how the circulant approach compares with familiar approaches to cubic and quartic equations. The novel perspective provided by circulants not only provides unified solutions of the equations, but also lends a new way to look at related questions, including elimination of the term of degree $n-1$ and characterizing equations with real roots. We conclude by placing the circulant approach in a general setting, and providing some examples of other matrix algebras, which, like the circulants, can be used to solve quartics.

**6. MATRIX ALGEBRAS AND POLYNOMIALS.** What is really going on in the circulant approach? One aspect is revealed by Sah's approach [**19**]. He defines the circulants by conjugating diagonal matrices with the fixed matrix $Q$. That is, he starts with a generic diagonal matrix $D$, and computes $QDQ^{-1}$. The resulting set of matrices is isomorphic to the matrix algebra of diagonal matrices. In particular, it is an $n$-dimensional linear space and given a basis, every element has a unique representation by means of $n$ coefficients. These coefficients are the parameters that must be determined when we use the circulants to solve an equation. Since the particular basis we use is $\{I, W, W^2, \ldots, W^{n-1}, \}$, linear combinations of the basis elements can also be viewed as polynomials in $W$.

The basis also provides a means for determining the eigenvalues of a general element of the matrix algebra. For a circulant matrix $C = q(W) = a_0 I + a_1 W + \cdots + a_{n-1}W^{n-1}$, (9) reveals a linear mapping of the coefficient vector $(a_0, a_1, \ldots, a_{n-1})$ into the eigenvalue vector $(r_1, r_2, \ldots, r_n)$. This situation arises for *any* basis of the matrix algebra. To see this let $\{C_1, C_2, \ldots, C_n\}$ be a basis for the matrix algebra as a linear space over the complex field, and express a generic element of the algebra as $C = \sum a_k C_k$. Consider one fixed column $v$ of $Q$, which is an eigenvector of every circulant matrix. In particular, $v$ is an eigenvector of each $C_k$; let the corresponding eigenvalue be $\lambda_k$. Then

$$Cv = \sum a_k C_k v = \sum a_k \lambda_k v,$$

so relative to $v$, $C$'s eigenvalue is $\sum \lambda_k a_k$. In this way, we express each eigenvalue of $C$ as a linear combination of the coefficients $a_k$. For the special basis $C_k = W^{k-1}$, the eigenvalues $\lambda_k$ become powers $v^k$ of a root of unity $v$, and the linear combination $\sum \lambda_k a_k$ equals $\sum a_k v^k$, which we interpreted as a polynomial in $v$.

The entire framework of Sah's development can be carried out in complete generality. Let $P$ be any nonsingular matrix. Define an algebra of matrices by conjugating all the diagonal matrices by $P$. A generic element of the algebra has the form $A = PDP^{-1}$, and in particular, has a complete set of eigenvectors defined by the columns of $P$. Also, viewing the algebra as a linear space, we may select a basis $\{A_1, A_2, \ldots, A_n\}$ and determine the set of eigenvalues for each basis element corresponding to the columns of $P$. Specifically, denoting column $i$ of $P$ as $v_i$, let $\lambda_{ij}$ be the corresponding eigenvalue for basis element $A_j$. That means

$$A_j v_i = \lambda_{ij} v_i.$$

Finally, consider a generic element of the algebra, expressed in terms of the basis as $A = \sum a_j A_j$. The eigenvalues of $A$ are the expressions $\sum \lambda_{ij} a_j$. That is, the vector of eigenvalues of $A$ is the product

$$\begin{bmatrix} \lambda_{11} & \lambda_{12} & \cdots & \lambda_{1n} \\ \lambda_{21} & \lambda_{22} & \cdots & \lambda_{2n} \\ \vdots & \vdots & & \vdots \\ \lambda_{n1} & \lambda_{n2} & \cdots & \lambda_{nn} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix},$$

which is the analog of (9). Therefore, once a member of the algebra has been expressed in terms of the basis, the eigenvalues can be obtained immediately using the coefficients $a_j$ and the matrix $[\lambda_{ij}]$.

Is it possible to use an arbitrary algebra defined in this way to derive solutions of the cubic and quartic equations? Let a polynomial $p$ be given. We must find an element $A$ of the matrix algebra such that $p$ is the characteristic polynomial of $A$. If the parameters $a_j$ are specified, the matrix $A$ and the eigenvalues are determined, so the characteristic polynomial can be computed. Now we have to invert that process: given the polynomial we need to determine the parameters.

Carrying out this step requires not only a suitable matrix $P$, but a particularly convenient choice for the basis, as well. In the one example we have examined, both are very special. Slightly modifying Sah's formulation, we can take $P = Q/\sqrt{n}$, which is both unitary and Hermitian. It is the DFT matrix. The basis, made up of the powers of $W$, is a cyclic group, so that the algebra of matrices is actually a group algebra. And while it is not clear how (or whether) these properties contribute to the invertibility of the parameter-to-characteristic-polynomial map, it is clear that the circulants are based on some very special matrices.

In the general case, given a $P$, we can compute a generic element of the algebra. The structure of that generic element may suggest a particularly convenient basis. The basis, in turn, determines the parameters that appear in the characteristic polynomial, as well as the matrix that maps parameters to eigenvalues.

The impact of this development on the equations that appear in the solution of the cubic and quartic can be understood as follows. The most direct attack on the problem of solving a polynomial equation is to invert the mapping from roots to coefficients. The components of this map are the elementary symmetric functions. The inversion process requires that we deduce the roots from the values of the elementary symmetric functions on the roots (i.e., from the coefficients). That amounts to solving a system of $n$ polynomial equations in $n$ variables, the roots. For example, if $p(x) = x^4 + \alpha x^3 + \beta x^2 + \gamma x + \delta$ has roots $r, s, t, u$ then

$$\begin{aligned} r + s + t + u &= -\alpha \\ rs + rt + ru + st + su + tu &= \beta \\ rst + rsu + rtu + stu &= -\gamma \\ rstu &= \delta. \end{aligned} \tag{11}$$

Regarding $r$, $s$, $t$, and $u$ as unknowns and $\alpha$, $\beta$, $\gamma$, and $\delta$ as given, solving this system of equations is equivalent to solving the general fourth degree equation.

In the context of the matrix algebra approach, we know that the roots are expressed as a linear transformation of the parameters. So, in effect, we make a linear change of variables in the arguments of the symmetric functions, and restate the system of equations (e.g., (11)) in terms of a new set of parameters. When the method works properly, these new equations are easier to solve than the original set.

The linear change of variables depends on the basis that is adopted. How should that basis be chosen? One possibility arises out of the conjugation process. Begin with

a natural basis for the diagonal matrices: $D_j$ is the diagonal matrix with a one in the $(j, j)$ position, and zeroes elsewhere. These diagonal matrices map to the basis $\{PD_jP^{-1} | 1 \leq j \leq n\}$ for the conjugate matrix algebra. However, for this choice of basis, the linear map from parameters to eigenvalues is the identity, and the matrix algebra approach leads to the same system of equations as direct inversion of the elementary functions ((11) in the quartic case). We mention this example to stress the fact that the most natural basis for the conjugate algebra is not necessarily the image of the natural basis of the diagonal matrix algebra. Indeed, *that* basis renders the matrix algebra approach to solving cubics and quartics completely ineffectual. What makes a basis for the conjugate algebra natural is the pattern of entries that appears in elements of the algebra. So, in the circulant algebra, there is an evident pattern of equal entries, and that pattern defines the natural basis. In other matrix algebra examples later in this section, a natural basis arises in a similar way.

At this point we should mention again Ungar's paper [**21**], which directly imposes a linear change of variables in the elementary symmetric functions. For example, in the case of the quartic, he introduces parameters $a, b, c, d$ related to the roots $r_j$ by the equation

$$\begin{bmatrix} r_1 \\ r_2 \\ r_3 \\ r_4 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix}.$$

This product expresses each root as a linear combination of the parameters. Substituting these expressions into the elementary symmetric functions results in a new system of polynomial equations that is quite readily solved. We discuss this system presently, but for now we merely observe that Ungar's approach is equivalent to the matrix algebra approach, and completely avoids the entire construction involving $P$. That is much more direct, assuming that one already knows what linear change of variables works. The matrix approach, in contrast, provides an attractive heuristic for finding suitable changes of variables.

**Klein Matrices.** As an example, working with the quartic, let us pick a particular choice of $P$ and see where it leads. (The trivial choice, $P = I$ leaves the parameters equal to the roots themselves, and so, requires direct inversion of the elementary symmetric functions.) We want a matrix that is as simple as possible, one with a simply determined inverse. One that comes to mind is

$$P = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}.$$

This $P$ is both symmetric and orthogonal, so that $P = P^T = P^{-1}$. Conjugating a diagonal matrix by $P$ produces something of the form

$$\begin{bmatrix} a & b & c & d \\ b & a & d & c \\ c & d & a & b \\ d & c & b & a \end{bmatrix}. \tag{12}$$

We refer to matrices of this form as *Klein matrices*.

It should be stressed that the general form for the Klein matrix (12) is *not* given by $PDP^{-1}$ where $D$ has $a, b, c, d$ on the diagonal. However, if a generic diagonal matrix is conjugated by $P$, the result follows the pattern of entries in (12): all the main diagonal entries are equal, all the cross diagonal entries are equal, and so on. This pattern of entries reveals a natural basis for the Klein matrices, and as discussed previously, it is fortunate that the natural basis does not correspond to the natural basis for the diagonal matrices.

As revealed in the pattern of entries, the natural basis for the Klein matrices is:

$$\left\{ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \right\}.$$

Following our earlier discussion, we can deduce from the basis and $P$ how the eigenvalues of a Klein matrix depend on the parameters $a$, $b$, $c$, and $d$. If we refer to the eigenvalues as $r$, $s$, $t$, and $u$, then

$$\begin{bmatrix} r \\ s \\ t \\ u \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix}. \tag{13}$$

There are several points to note. First, the transformation from parameters to eigenvalues is just a multiple of the matrix $P$. This is not something that occurs in general, although it is a common feature of Klein and circulant matrices. Second, as (13) makes clear, using the Klein matrices leads to precisely the change of variables prescribed by Ungar. Thus, Ungar's method arises in a natural way when the matrix heuristic is used. Third, as is the case for circulant matrices, the Klein matrices have a lot of structure. The basis elements again form a group, this time the Klein four group, revealing the inspiration for the name *Klein matrices*. This group is a direct product of two cyclic groups, and in the same way the Klein matrices can be expressed as a Kronecker (tensor) product of two two-dimensional matrix algebras, namely, the two dimensional circulant algebra with generic element

$$\begin{bmatrix} a & b \\ b & a \end{bmatrix}.$$

The Kronecker product of two matrices $A$ and $B$ is formed as follows: beside each entry of $A$ place a complete copy of $B$, thus forming a partitioned matrix whose blocks are scalar multiples of $B$. The Klein matrices can be obtained by forming Kronecker products of $2 \times 2$ circulants, and then forming all possible sums. Indeed, this block Kronecker structure is revealed quite clearly by partitioning Klein matrices into $2 \times 2$ submatrices. Thus, the structure of the Klein matrices as a group algebra reflects the structure of the Klein group in a natural way. Finally, it is interesting to observe that ignoring the normalization factor $1/2$, $P$ is a *Hadamard matrix*. Hadamard matrices have many applications in signal processing and combinatorics; see [**1**], [**10**], and [**18**] for some samples. Among other things, Hadamard matrices are used to define the *Hadamard transform*, which is a kind of binary analogue of the DFT.

What does the solution of the quartic look like using Klein matrices? As before, we consider only reduced quartics, of the form $p(x) = x^4 + \beta x^2 + \gamma x + \delta$. These correspond to Klein matrices with vanishing main diagonal. Therefore, we need to

consider only Klein matrices of the form

$$\begin{bmatrix} 0 & b & c & d \\ b & 0 & d & c \\ c & d & 0 & b \\ d & c & b & 0 \end{bmatrix}.$$

The characteristic polynomial of this matrix is

$$x^4 - 2(b^2 + c^2 + d^2)x^2 - 8(bcd)x + b^4 + c^4 + d^4 - 2(b^2c^2 + b^2d^2 + c^2d^2).$$

Therefore, equating the coefficients of the characteristic polynomial with those of $p$, we obtain the system

$$\begin{aligned} b^2 + c^2 + d^2 &= -\beta/2 \\ bcd &= -\gamma/8 \\ b^4 + c^4 + d^4 - 2(b^2c^2 + b^2d^2 + c^2d^2) &= \delta. \end{aligned} \tag{14}$$

This is the same system of equations that Ungar's method produces, so from this point on, our analysis repeats his.

The system (14) features symmetric functions of the parameters $b^2$, $c^2$, and $d^2$. To exploit these symmetries, rewrite the last equation of (14) in the form

$$(b^2 + c^2 + d^2)^2 - 4(b^2c^2 + b^2d^2 + c^2d^2) = \delta.$$

Now we can use the first equation to eliminate $(b^2 + c^2 + d^2)$ from the third equation, and square the second, leading to

$$\begin{aligned} b^2 + c^2 + d^2 &= -\frac{\beta}{2} \\ b^2c^2d^2 &= \frac{\gamma^2}{64} \\ b^2c^2 + b^2d^2 + c^2d^2 &= \frac{\beta^2}{16} - \frac{\delta}{4}. \end{aligned} \tag{15}$$

Here we see the elementary symmetric polynomials in three indeterminates, acting on $b^2$, $c^2$, and $d^2$. This shows at once that $b^2$, $c^2$, and $d^2$ are the zeroes of the cubic polynomial

$$x^3 + \frac{\beta}{2}x^2 + \left(\frac{\beta^2}{16} - \frac{\delta}{4}\right)x - \frac{\gamma^2}{64},$$

so that $b$, $c$, and $d$ are simply the square roots of these zeroes. And the roots of the original quartic are combinations of $b$, $c$, and $d$ (and $a = 0$) according to (13). Interestingly, this parameterization of the roots of the quartic is equivalent to a solution by Euler [**6**, pp. 104–107].

As this analysis shows, in deriving the solution to the quartic, using Klein matrices is easier than using circulant matrices. Although both approaches require solving the same resolvant cubic, in the Klein approach the roots of this cubic lead more directly

to the required parameters $b$, $c$, and $d$ (just take square roots), and the roots of the original quartic are found by simply adding and subtracting the parameters.

In this formulation, the determination of conditions for real roots is also particularly simple. The equations linking the parameters and the roots show that all the roots are real if and only if all the parameters are real. Since the parameters are square roots of the zeroes of the resolvant cubic, they are all real just in case that cubic has three nonnegative roots. This is the same result found before, but this time with a much simpler derivation. Moreover, we can now continue the analysis to derive conditions directly on the coefficients $\beta$, $\gamma$, and $\delta$. Assume first that all roots of the original quartic are real. Then the resolvant cubic likewise has only real roots. Performing the linear shift to eliminate the square term, and imposing our earlier result regarding real roots of cubics, we find that

$$\delta(\beta^2 - 4\delta)^2 + \gamma^2\left(9\beta\delta - \frac{\beta^3}{4} - \frac{27\gamma^2}{16}\right) \geq 0.$$

In addition, since the roots of the quartic are real so are $b$, $c$, and $d$; their squares are therefore nonnegative. Combining this observation with (15) reveals that $\beta \leq 0$ and $\beta^2/4 \geq \delta$. Thus we have three necessary conditions on the coefficients of $p$ when all roots are real.

These conditions are also sufficient. If the first condition holds, then the resolvant cubic has three real roots. The other two conditions ensure that the coefficients of the resolvant cubic alternate in sign, thus forbidding the existence of a real negative root. Together, these inferences show that the three roots of the resolvant cubic are all nonnegative. That leads in turn to real values of parameters $b$, $c$, and $d$, and hence implies that the roots of $p$ are all real.

The Klein matrices offer an amazingly simple algebraic solution of the quartic. The parameterization is particularly suitable for characterizing the case of all real roots. On the other hand, circulant matrices offer a unified approach to cubic and quartic equations, while Klein matrices only work for quartics. Thus, each matrix algebra has something to offer.

It is certainly natural to wonder whether another matrix algebra might contribute still other ideas. We have examined several possibilities. In some cases, the equations that are derived for the parameters are too complicated to inspire much effort toward a solution. In a few other cases, we have rediscovered earlier parameterizations in a new guise. Indeed, a given basis can be mapped from one algebra to another by composing conjugations, without altering the eigenvalues. Thus, although this mapping may give the appearance of introducing a new matrix algebra, the underlying linear change of variables remains the same, and so ultimately the same system of equations must specify the parameters.

We have discovered one matrix algebra that does provide a new parameterization and has some interesting additional aspects. We conclude the paper by outlining this example.

**Cartesian Matrices.** For this example, we define

$$P = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}.$$

As before, $P = P^T = P^{-1}$, and $P$ exhibits an obvious block structure.

The image of the diagonal matrices under conjugation can be expressed in the form

$$E = \begin{bmatrix} r & s & 0 & 0 \\ s & r & 0 & 0 \\ 0 & 0 & u & t \\ 0 & 0 & t & u \end{bmatrix}. \tag{16}$$

We call matrices of the form (16) *Cartesian matrices*.

Assuming as always that the trace vanishes, we see that $u = -r$, so

$$E = \begin{bmatrix} r & s & 0 & 0 \\ s & r & 0 & 0 \\ 0 & 0 & -r & t \\ 0 & 0 & t & -r \end{bmatrix}.$$

The eigenvalues are then given by $r + s$, $r - s$, $-r + t$, and $-r - t$. This immediately reveals that the characteristic polynomial for $E$ is

$$\begin{aligned} p(x) &= (x - r - s)(x - r + s)(x + r - t)(x + r + t) \\ &= [(x - r)^2 - s^2][(x + r)^2 - t^2]. \end{aligned} \tag{17}$$

Thus this parameterization imposes a decomposition of the quartic into two quadratic factors. This is reminiscent of Descartes' solution of the quartic [**3**, p. 136], and inspires the name *Cartesian matrices*. Expanding the right side of (17), and matching coefficients with the standard quartic $x^4 + \beta x^2 + \gamma x + \delta$ produces the system

$$\begin{aligned} s^2 + t^2 + 2r^2 &= -\beta \\ 2r(t^2 - s^2) &= \gamma \\ (r^2 - s^2)(r^2 - t^2) &= \delta. \end{aligned}$$

To solve these equations, use the first two to express $s^2 + t^2$ and $s^2 - t^2$ in terms of $r$ and the coefficients $\beta$, $\gamma$, $\delta$. That in turn permits $s^2$ and $t^2$ to be isolated, and hence eliminated from the final equation. That produces, once again, the resolvant cubic, this time as a polynomial in $r^2$. Any solution $r^2$ gives rise to values of $r$, $s$, and $t$, and hence to the roots of the original quartic.

Here, then, is another parameterization for solving the quartic. In contrast to the two previous examples, the *natural* basis for the Cartesian matrices does not constitute a group, so it does not give rise to a group algebra. Although the algebraic solution of the quartic by the method of Cartesian matrices is no simpler than by the method of Klein matrices, it is interesting to see how the resolvant cubic appears again, and to compare the methods. It is also interesting that one approach reproduces a solution of Euler, while the other is similar to a solution of Descartes.

It may be that other matrix algebras give rise to new parameterizations of the quartic. In particular, it would be interesting to see if the original solution of the quartic due to Ferrari can be obtained using a suitable matrix algebra.

REFERENCES


1. Stephen Barnett, *Matrices Methods and Applications*, Oxford University Press, New York, 1990.
2. W. G. Bridges and R. A. Mena, Rational circulants with rational spectra and cyclic strongly regular graphs, *Ars Combin.* (1979) 143–161.
3. William Snow Burnside and Arthur William Panton, *The Theory of Equations*, Vol. 1, 7th ed., Dublin University Press, Dublin, 1912.

4. Ronald Calinger, ed., *Classics of Mathematics*, Moore Publishing, Oak Park, Illinois, 1982.
5. Philip Davis, *Circulant Matrices*, Wiley, New York, 1979.
6. William Dunham, *Euler The Master of Us All*, Mathematical Association of America, Washington, DC, 1999.
7. John Fauvel and Jeremy Gray, eds., *The History of Mathematics—A Reader*, MacMillan Education LTD, London, 1987.
8. Orrin Frink Jr., A method for solving the cubic, *Amer. Math. Monthly* **32** (1925) 134.
9. Joseph A. Gallian, *Contemporary Abstract Algebra*, 3rd ed., Heath, Lexington, MA, 1994.
10. Solomon W. Golomb and Leonard D. Baumert, The search for Hadamard matrices, *Amer. Math. Monthly* **70** (1963) 12–17.
11. Jan Gullberg, *Mathematics from the Birth of Numbers*, W. W. Norton, New York, 1997.
12. Morton J. Hellman, A unifying technique for the solution of the quadratic, cubic, and quartic, *Amer. Math. Monthly* **65** (1959) 274–276.
13. Dan Kalman and James White, A simple solution of the cubic, *College Math. J.* **29** (1998) 415–418.
14. Victor J. Katz, *A History of Mathematics—an Introduction*, Harper Collins, New York, 1993.
15. R. Bruce King, *Beyond the Quartic Equation*, Birkhäuser, Boston, 1996.
16. Morris Kline, *Mathematical Thought from Ancient to Modern Times*, Oxford University Press, New York, 1972.
17. E. J. Oglesby, Note on the algebraic solution of the cubic, *Amer. Math. Monthly* **30** (1923) 321–323.
18. W. K. Pratt, J. Kane, and H. C. Andrews, Hadamard transform image coding, *Proc. IEEE* **57** (1969) 58–68.
19. A. Pen-Tung Sah, A uniform method of solving cubics and quartics, *Amer. Math. Monthly* **52** (1945) 202–206.
20. Robert Y. Suen, Roots of cubics via determinants, *College Math. J.* **25** (1994) 115–117.
21. Abraham A. Ungar, A unified approach for solving quadratic, cubic, and quartic equations by radicals, *Int. J. Comp. Math. Appl.* **19** (1990) 33–39.
22. B. L. van der Waerden, *Algebra*, Vol. 1, translated by Fred Blum and John Schulenberger, Frederick Ungar, New York, 1970.
23. C. R. White, Definitive solutions of general quartic and cubic equations, *Amer. Math. Monthly* **69** (1962) 285–287.
24. James E. White, Cubic Equations (a Mathwright workbook), *The New Mathwright Library*, http://www.mathwright.com/book_pgs/book241.html.
25. James E. White, Cardano (a LAVA workbook viewable as a webpage), *The New Mathwright Library*, http://www.mathwright.com/lr_lavapage.html.

**DAN KALMAN** received his Ph.D. from the University of Wisconsin in 1980. He joined the mathematics faculty at American University in 1993, following an eight-year stint in the aerospace industry and earlier teaching positions in Wisconsin and South Dakota. Kalman has won three MAA writing awards, is a past associate editor of *Mathematics Magazine*, and served a term as Associate Executive Director of the MAA. His interests include matrix algebra, curriculum development, and interactive computer environments for exploring mathematics, especially using Mathwright software.
*Department of Mathematics and Statistics, American University, 4400 Massachusetts Avenue NW, Washington, DC 20016-8050*
*kalman@american.edu*

**JAMES WHITE** received his Ph.D. in mathematics from Yale University in 1972. He has held teaching positions in mathematics at the University of California, San Diego, Carleton College, and Bates College, and has had research positions in computer science at the Jet Propulsion Lab in Pasadena, and at the University of North Carolina, Chapel Hill. He led the development team for IBM's ToolKit for Interactive Mathematics (TIM) and is the author of several other computer languages, including Mathwright, Lava, and MindScapes. White was co-director of the MAA's Interactive Mathematics Text Project, and is the principal investigator for the current MAA Project WELCOME. He is the developer, and is now the chief librarian, of The New Mathwright Library and Cafe, an internet library at http://www.mathwright.com.
*33641 Hartford Drive, Union City, CA 94587*
*mathwrig@gte.net*