Polynomial Equations and Circulant Matrices

Dan Kalman, American University
James White, Bluejay Lispware

Forthcoming Monthly article: November 2001, pp 821 - 840

Preprint (pdf): www.dankalman.net/preprints
Find link for circulant.pdf

Outline

- Circulant Matrices
- Solving the Cubic and Quartic
- Another View: Conjugation and Diagonal Matrices
- Other Matrix Algebras

Circulant Matrices

- Example, 3×3

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

- Example, 4×4

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

- Circulants arise naturally in many applications, including signal processing and graph theory, have many interesting properties

Eigenvalues and Eigenvectors

- Consider a circulant with first row $[c_0 \;\; c_1 \;\; c_2 \;\; \cdots \;\; c_{n-1}]$
- Define $q(t) = c_0 + c_1 t + c_2 t^2 + \cdots + c_{n-1} t^{n-1}$
- Eigenvalues are $q(\omega)$ where ω is an nth root of unity
- Eigenvectors have form $v_\omega = [1 \;\; \omega \;\; \omega^2 \;\; \cdots \;\; \omega^{n-1}]^T$
- Eigenvalues can be read off by inspection

Example

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

$\omega \in \{1, -1, i, -i\}$

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

eigenvalues	eigenvectors
$q(1) = 6$	$v_1 = (1, 1, 1, 1)$
$q(-1) = -3$	$v_{-1} = (1, -1, 1, -1)$
$q(i) = -i$	$v_i = (1, i, -1, -i)$
$q(-i) = i$	$v_{-i} = (1, -i, -1, i)$

Note: characteristic polynomial of C is $p(t) = t^4 - 4t^3 - 20t^2 - 4t - 21$

Another Example

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

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

$$\omega \in \left\{ 1, \frac{-1 + i\sqrt{3}}{2}, \frac{-1 - i\sqrt{3}}{2} \right\}$$

Eigenvalues: $1 + \sqrt[3]{2} + \sqrt[3]{4}$, $1 - (\frac{1}{2})\sqrt[3]{2} - (\frac{1}{2})\sqrt[3]{4} \pm (\frac{1}{2})i\sqrt{3}(\sqrt[3]{4} - \sqrt[3]{2})$.
Characteristic polynomial: $p(t) = t^3 - 3t^2 - 3t - 1$.

Another View

- Generator W: circulant with first row $[0 \;\; 1 \;\; 0 \;\; \cdots \;\; 0]$

$$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

- W is Identity matrix with top row shifted to the bottom
- General circulant: $q(W)$ where q is a polynomial of degree one less than the dimension of W.
- For 3×3 W : $aI + bW + cW^2$

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

Explanation of Eigen - Info

- Minimal/characteristic polynomial for W : $W^n - 1$
- Eigenvalues of W : n^{th} roots of unity ω
- Eigenvalues of $q(W)$ are $q(\omega)$

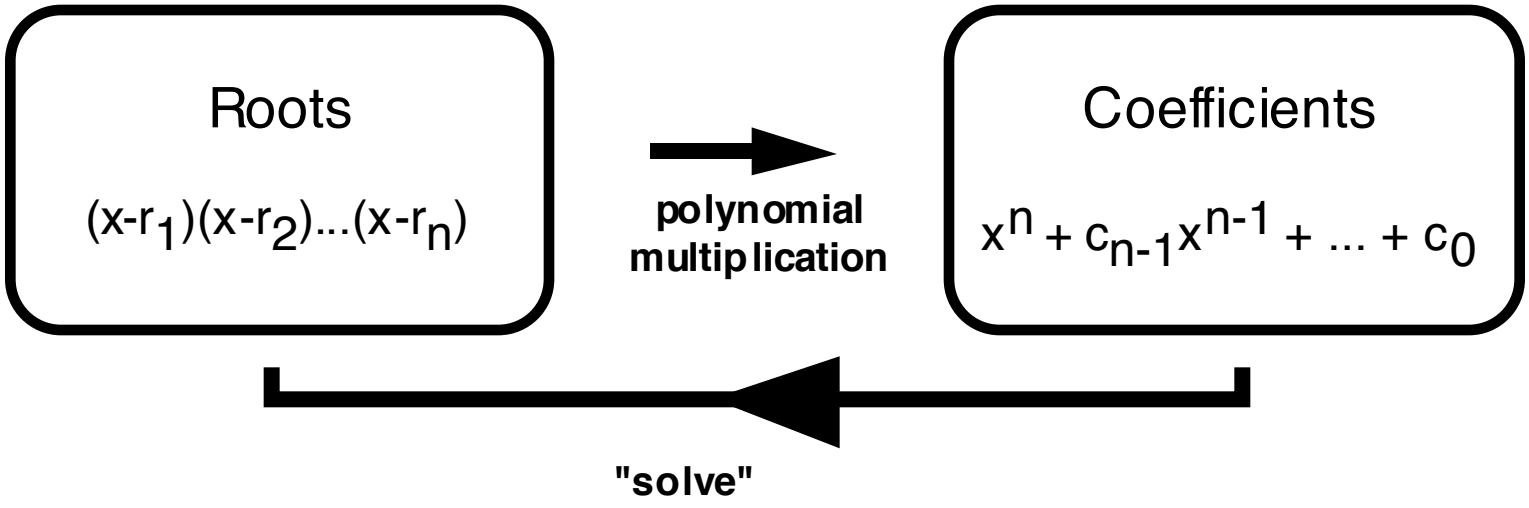
$$W\mathbf{v} = \omega\mathbf{v} \Rightarrow q(W)\mathbf{v} = q(\omega)\mathbf{v}$$

- Eigenvalues of $aI + bW + cW^2$ are $a + b\omega + c\omega^2$ where ω is any 3^{rd} root of unity

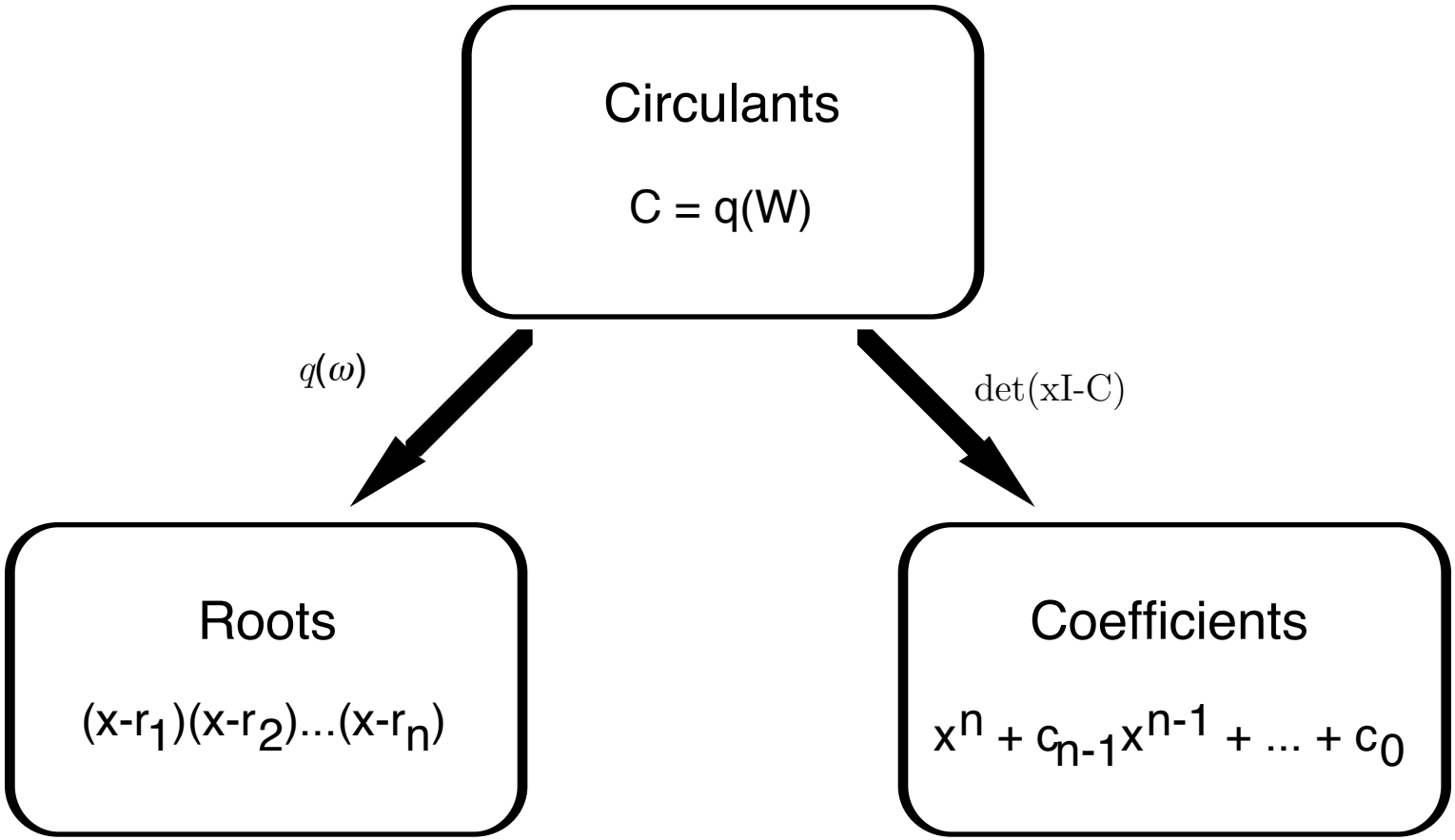
Solving Polynomials with Circulants

- Usual notion of solving a polynomial: given coefficients, find roots
- Circulants give us a rich set of polynomials with known roots
- New approach to solving a polynomial: given p (defined in terms of coefficients), find a circulant matrix $C = q(W)$ for which p is the characterisic polynomial. The eigenvalues $q(\omega)$ of C are then the roots of p

Usual Method



Circulant Method



Example

- $p(t) = t^3 - 3t^2 - 3t - 1$
- p is the characteristic polynomial of $C = \begin{bmatrix} 1 & \sqrt[3]{2} & \sqrt[3]{4} \\ \sqrt[3]{4} & 1 & \sqrt[3]{2} \\ \sqrt[3]{2} & \sqrt[3]{4} & 1 \end{bmatrix}$
- By inspection, eigenvalues are $q(\omega) = 1 + \omega\sqrt[3]{2} + \omega^2\sqrt[3]{4}$ where ω is a cuberoot of unity
- This gives the roots of p

Finding the right Circulant

- Given monic p of degree n, find a circulant matrix $C(p)$ for which the characteristic polynomial is p
- $C(p) = q(W)$ for an appropriate polynomial q of degree $n-1$
- Existence: if the roots of p are r_k, and the n^{th} roots of unity are ω_k, it suffices to have $q(\omega_k) = r_k$. Existence of q assured by polynomial interpolation theory.

Another View

Let $q(x) = q_0 + q_1 x + \cdots + q_{n-1}x^{n-1}$. Let the roots of p be r_k for $1 \leq k \leq n$. Let $\omega = e^{2\pi i/n}$, so that the powers of ω are the n^{th} roots of unity. Then q maps the roots of unity to the r_k if

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \cdots & \omega^{(n-1)(n-1)} \end{bmatrix} \begin{bmatrix} q_0 \\ q_1 \\ q_2 \\ \vdots \\ q_{n-1} \end{bmatrix} = \begin{bmatrix} r_1 \\ r_2 \\ r_3 \\ \vdots \\ r_n \end{bmatrix}$$

This system is easily seen to be solvable for any choice of the r_k. **Side Comment:** The column of r_k is the discrete fourier transform of the column of q_j.

Recap

- Preceding arguments show that **any** monic degree n polynomial can be realized as the characteristic polynomial for some circulant matrix $q(W)$
- We do not know the roots r_k
- Need an alternate way to find q
- Then we can compute the roots by applying q to roots of unity
- Next step: compute a generic circulant characteristic polynomial

Traceless Circulants

- WLOG the degree $n-1$ term of p vanishes
- Equivalently, sum of roots of p vanishes
- Equivalently, sum of eigenvalues of $q(W)$ vanishes
- Equivalently, trace of $q(W)$ vanishes
- Equivalently, diagonal of $q(W)$ vanishes

Characteristic Polynomial

$$\det(xI - M) = \det \begin{bmatrix} x & -q_1 & -q_2 & \cdots & -q_{n-1} \\ -q_{n-1} & x & -q_1 & \cdots & -q_{n-2} \\ -q_{n-2} & -q_{n-1} & x & \cdots & -q_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -q_1 & -q_2 & -q_3 & \cdots & x \end{bmatrix}$$

CONCLUSION: General formula for the determinant of a circulant suffices.

Case $n = 3$

The characteristic polynomial of $M = q(W) = q_1 W + q_2 W^2$:

$$\begin{aligned}
\det\left(xI - \begin{bmatrix} 0 & q_1 & q_2 \\ q_2 & 0 & q_1 \\ q_1 & q_2 & 0 \end{bmatrix}\right) &= \det\begin{bmatrix} x & -q_1 & -q_2 \\ -q_2 & x & -q_1 \\ -q_1 & -q_2 & x \end{bmatrix} \\
&= x^3 - q_1^3 - q_2^3 - 3q_1q_2x \\
&= x^3 - 3q_1q_2x - (q_1^3 + q_2^3)
\end{aligned}$$

Solving the Cubic

- Given $p(x) = x^3 + ax + b$
- Characteristic polynomial of $q(W)$ is $x^3 - 3q_1q_2x - (q_1^3 + q_2^3)$
- Must solve the system

$$\begin{aligned} q_1^3 + q_2^3 &= -b \\ q_1 q_2 &= -a/3 \end{aligned}$$

- Roots of p will be $q(1) = q_1 + q_2$, $q(\omega) = q_1\omega + q_2\omega^2$, and $q(\omega^2) = q_1\omega^2 + q_2\omega$ where $\omega = \dfrac{-1 + i\sqrt{3}}{2}$

Finding q

$$\left\{ \begin{array}{rcl} q_1^3 + q_2^3 & = & -b \\ q_1 q_2 & = & -a/3 \end{array} \right\} \Rightarrow \left\{ \begin{array}{rcl} q_1^3 + q_2^3 & = & -b \\ q_1^3 q_2^3 & = & -a^3/27 \end{array} \right\}$$

q_1^3 and q_2^3 are roots of $x^2 + bx - a^3/27 = 0$

Thus, q_1 and q_2 are given by

$$\left\{ \frac{-b \pm \sqrt{b^2 + 4a^3/27}}{2} \right\}^{1/3} \quad \text{or} \quad \left\{ \frac{-b}{2} \pm \sqrt{\frac{b^2}{4} + \frac{a^3}{27}} \right\}^{1/3}$$

Solving the Quartic

- $x^4 + ax^2 + bx + c$
- Characteristic polynomial of $q(W)$

  $$x^4 - (4q_3q_1 + 2q_2^2)x^2 - 4q_2(q_1^2 + q_3^2)x + (q_2^4 - q_1^4 - q_3^4 - 4q_1q_3q_2^2 + 2q_1^2q_3^2) = 0$$

- Elimination leads to

  $$q_2^6 + \frac{a}{2}q_2^4 + \left(\frac{a^2}{16} - \frac{c}{4}\right)q_2^2 - \frac{b^2}{64} = 0$$

- 4th roots of unity: $\pm 1, \pm i$
- Roots of p: $\pm q_1 + q_2 \pm q_3$, and $\pm iq_1 - q_2 \mp iq_3$.

Quintic and Beyond

- For any n, the nth roots of unity are expressible in terms of radicals
- Suppose p is a polynomials whose roots r_k are *not* expressible in terms of radicals (possible for degree 5 or more according to Galois Theory)
- If $q(W)$ is a circulant having p as characteristic polynomial, then each r_k is a linear combination of roots of unity and coefficients of q.
- Since the roots of unity are expressible in terms of radicals, the coefficients of q *cannot* be.
- Circulant Method Fails

Another View

- First view: polynomials in a generator W
- New view: $\{QDQ^{-1}|D$ any diagonal matrix$\}$
- Q is a fixed matrix (of eigenvectors)
- New view gives alternate explanation of eigen-info
- Provides obvious way to generalize to new matrix algebras
- General method reduces to making a linear change of variables in the root finding problem
- There are connections with historical solutions of quartic

Conjugation

- Reference: A. Pen-Tung Sah, *A uniform method of solving cubics and quartics,* **Amer. Math. Monthly** 52 (1945) 202–206.
- Let Q be the matrix of eigenvectors v_ω
- For any diagonal D define corresponding matrix $C(D) = QDQ^{-1}$
- This mapping is clearly an isomorphism from the algebra of diagonal matrices onto its image – the *Conjugate Algebra*
- This image algebra turns out to be the circulants
- Every matrix in the conjugate algebra is clearly diagonalized by the same matrix: $Q^{-1}CQ = D$

Conjugate a Generic Diagonal Matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix} \begin{bmatrix} \alpha & 0 & 0 & 0 \\ 0 & \beta & 0 & 0 \\ 0 & 0 & \gamma & 0 \\ 0 & 0 & 0 & \delta \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix}^{-1} =$$

$$\frac{1}{4} \begin{bmatrix} \alpha+\beta+\gamma+\delta & \alpha-\gamma-i(\beta-\delta) & \alpha-\beta+\gamma-\delta & \alpha-\gamma+i(\beta-\delta) \\ \alpha-\gamma+i(\beta-\delta) & \alpha+\beta+\gamma+\delta & \alpha-\gamma-i(\beta-\delta) & \alpha-\beta+\gamma-\delta \\ \alpha-\beta+\gamma-\delta & \alpha-\gamma+i(\beta-\delta) & \alpha+\beta+\gamma+\delta & \alpha-\gamma-i(\beta-\delta) \\ \alpha-\gamma-i(\beta-\delta) & \alpha-\beta+\gamma-\delta & \alpha-\gamma+i(\beta-\delta) & \alpha+\beta+\gamma+\delta \end{bmatrix}$$

A basis For The Conjugate Algebra

Define

$$\begin{aligned} a &= (\alpha+\beta+\gamma+\delta)/4 \\ b &= (\alpha-\gamma-i(\beta-\delta))/4 \\ c &= (\alpha-\beta+\gamma-\delta))/4 \\ d &= (\alpha-\gamma+i(\beta-\delta)/4 \end{aligned}$$

Then

$$QDQ^{-1} = \begin{bmatrix} a & b & c & d \\ d & a & b & c \\ c & d & a & b \\ b & c & d & a \end{bmatrix}$$

This reveals a *natural* basis for the conjugate algebra:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Basis Coefficients Vs. Diagonal Elements

- Diagonal elements of D = eigenvalues = roots of p: $\alpha, \beta, \gamma, \delta$
- Coefficients of natural basis elements for QDQ^{-1}: a, b, c, d

$$\frac{1}{4}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{bmatrix}\begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix} = \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix}\begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix}$$

Circulant Method Revisited

- Given coefficients of p, we wish to find roots
- Instead, we find coefficients a, b, c, d for a corresponding circulant
- The roots are then found by inverting a linear system
- Equivalent to making the linear change of variables from $\alpha, \beta, \gamma, \delta$ to a, b, c, d

Elementary Symmetric Functions

If the roots are $\alpha, \beta, \gamma, \delta$, then the coefficients of p are given by

$$\begin{aligned} c_0 &= \alpha\beta\gamma\delta \\ c_1 &= -\alpha\beta\gamma - \alpha\beta\delta - \alpha\gamma\delta - \beta\gamma\delta \\ c_2 &= +\alpha\beta + \alpha\gamma + \alpha\delta + \beta\gamma + \beta\delta + \gamma\delta \\ c_3 &= -\alpha - \beta - \gamma - \delta \end{aligned}$$

Introducing the linear change of variables to a, b, c, d leads to the system of equations originally found in the circulant method

Generalizations

- Pick a different matrix for Q with nice properties
- Simple, real entries
- Inverse = transpose
- Hope for a nice natural basis
- Hope MATRIX $\rightarrow$ CHARACTERISTIC POLYNOMIAL is easy to invert

- Trivial case: $Q = I$ is equivalent to direct inversion of the symmetric function equations

Hadamard Matrix

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

Note $Q^{-1} = Q = Q^T$

Natural Basis

Conjugating a generic diagonal D using this Q results in a matrix with the pattern

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

revealing the natural basis

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

This basis is the Klein 4-group; I call these Klein matrices.

Basis Coefficients Vs. Eigenvalues

$$\frac{1}{4}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}\begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix} = \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}\begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix}$$

Revisiting the Quartic

- Given quartic $p(x) = x^4 + rx^2 + sx + t$
- Want to find Klein matrix, with coefficients $a = 0, b, c, d$ having p for characteristic polynomial.
- Must solve:

$$\begin{aligned} b^2 + c^2 + d^2 &= -\frac{r}{2} \\ b^2c^2d^2 &= \frac{s^2}{64} \\ b^2c^2 + b^2d^2 + c^2d^2 &= \frac{r^2}{16} - \frac{t}{4} \end{aligned}$$

- b^2, c^2, d^2 roots of the cubic

$$x^3 + \frac{r}{2}x^2 + \left(\frac{r^2}{16} - \frac{t}{4}\right)x - \frac{s^2}{64}$$

- This is Euler's solution of the quartic

One More Q

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

Note again $Q^{-1} = Q = Q^T$

Conjugate Algebra

Conjugating a diagonal D with zero trace, this Q results in a matrix with the pattern

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

By inspection, eigenvalues are $a \pm b$ and $-a \pm c$.

Proceeding as before, it is possible to derive another solution to the quartic. This time it is nearly the same as the solution of Descartes.

Final Comments

- Circulant method applies uniformly to quadratic, cubic, and quartic cases. Cubic solution is the same as Cardano's. Quartic solutions appears to be new, but is algebraically complicated
- Klein matrices apply only to quartic, but give algebraically simplest solution
- Main idea of all solutions: linear change of variables in the symmetric function equations
- Matrix conjugation approach provides a nice heuristic for finding suitable changes of variables
- Many additional interesting connections between matrices and polynomials discussed in the paper