# Solving polynomial equations with circulant matrix theory

Emanuel G. Indrei

MSRI

November 5, 2013

Solve: $z^n = 1$ for $n \in \mathbb{N}$.

- Recall that a complex number $z = x + iy \in \mathbb{C}$ may be written as $z = re^{i\theta}$, where $e^{i\theta} = cos(\theta) + isin(\theta)$.
- Here $r = |z| = \sqrt{x^2 + y^2}$ and $\theta = \theta_0 + 2\pi k, k \in \mathbb{Z}$.
- If $z^n = 1$, then $r = 1$. Now note that for each $k \in \mathbb{Z}$, $1 = e^{i2\pi k}$; so $z = e^{i\frac{2\pi k}{n}}$ solves $z^n = 1$.
- Let $\omega := e^{i\frac{2\pi}{n}}$. Then the distinct roots of unity are $\omega^k = e^{i\frac{2\pi k}{n}}$ for $k = 0, 1, \ldots, n-1$.

# Preliminaries: Roots of unity.

Solve: $z^n = 1$ for $n \in \mathbb{N}$.

- Recall that a complex number $z = x + iy \in \mathbb{C}$ may be written as $z = re^{i\theta}$, where $e^{i\theta} = cos(\theta) + isin(\theta)$.
- Here $r = |z| = \sqrt{x^2 + y^2}$ and $\theta = \theta_0 + 2\pi k, k \in \mathbb{Z}$.
- If $z^n = 1$, then $r = 1$. Now note that for each $k \in \mathbb{Z}$, $1 = e^{i2\pi k}$; so $z = e^{i\frac{2\pi k}{n}}$ solves $z^n = 1$.
- Let $\omega := e^{i\frac{2\pi}{n}}$. Then the distinct roots of unity are $\omega^k = e^{i\frac{2\pi k}{n}}$ for $k = 0, 1, \ldots, n-1$.

Solve: $z^n = 1$ for $n \in \mathbb{N}$.

- Recall that a complex number $z = x + iy \in \mathbb{C}$ may be written as $z = re^{i\theta}$, where $e^{i\theta} = cos(\theta) + isin(\theta)$.
- Here $r = |z| = \sqrt{x^2 + y^2}$ and $\theta = \theta_0 + 2\pi k, k \in \mathbb{Z}$.
- If $z^n = 1$, then $r = 1$. Now note that for each $k \in \mathbb{Z}$, $1 = e^{i2\pi k}$; so $z = e^{i\frac{2\pi k}{n}}$ solves $z^n = 1$.
- Let $\omega := e^{i\frac{2\pi}{n}}$. Then the distinct roots of unity are $\omega^k = e^{i\frac{2\pi k}{n}}$ for $k = 0, 1, \ldots, n-1$.

# Preliminaries: Roots of unity.

Solve: $z^n = 1$ for $n \in \mathbb{N}$.

- Recall that a complex number $z = x + iy \in \mathbb{C}$ may be written as $z = re^{i\theta}$, where $e^{i\theta} = cos(\theta) + isin(\theta)$.
- Here $r = |z| = \sqrt{x^2 + y^2}$ and $\theta = \theta_0 + 2\pi k, k \in \mathbb{Z}$.
- If $z^n = 1$, then $r = 1$. Now note that for each $k \in \mathbb{Z}$, $1 = e^{i2\pi k}$; so $z = e^{i\frac{2\pi k}{n}}$ solves $z^n = 1$.
- Let $\omega := e^{i\frac{2\pi}{n}}$. Then the distinct roots of unity are $\omega^k = e^{i\frac{2\pi k}{n}}$ for $k = 0, 1, \ldots, n-1$.

# Preliminaries: Roots of unity.

Solve: $z^n = 1$ for $n \in \mathbb{N}$.

- Recall that a complex number $z = x + iy \in \mathbb{C}$ may be written as $z = re^{i\theta}$, where $e^{i\theta} = cos(\theta) + isin(\theta)$.
- Here $r = |z| = \sqrt{x^2 + y^2}$ and $\theta = \theta_0 + 2\pi k, k \in \mathbb{Z}$.
- If $z^n = 1$, then $r = 1$. Now note that for each $k \in \mathbb{Z}$, $1 = e^{i2\pi k}$; so $z = e^{i\frac{2\pi k}{n}}$ solves $z^n = 1$.
- Let $\omega := e^{i\frac{2\pi}{n}}$. Then the distinct roots of unity are $\omega^k = e^{i\frac{2\pi k}{n}}$ for $k = 0, 1, \ldots, n-1$.

# Preliminaries: Eigenvalues and Eigenvectors.

- Let $A$ be an $n \times n$ matrix.
- An eigenvalue of $A$ is a number $\lambda$ such that there exists a non-zero vector $v \in \mathbb{R}^n$ for which $Av = \lambda v$.
- Since $(\lambda Id - A)0 = 0$, if $v$ is an eigenvector of $A$, then $\lambda Id - A$ is not $1 - 1$.
- In linear algebra language, this is expressed by saying $det(\lambda Id - A) = 0$.
- The previous formula expresses a method to find the eigenvalues of a given matrix $A$.
- Eigenvalues and eigenvectors have important applications throughout all of mathematics.

- Let $A$ be an $n \times n$ matrix.
- An eigenvalue of $A$ is a number $\lambda$ such that there exists a non-zero vector $v \in \mathbb{R}^n$ for which $Av = \lambda v$.
- Since $(\lambda Id - A)0 = 0$, if $v$ is an eigenvector of $A$, then $\lambda Id - A$ is not $1-1$.
- In linear algebra language, this is expressed by saying $det(\lambda Id - A) = 0$.
- The previous formula expresses a method to find the eigenvalues of a given matrix $A$.
- Eigenvalues and eigenvectors have important applications throughout all of mathematics.

# Preliminaries: Eigenvalues and Eigenvectors.

- Let $A$ be an $n \times n$ matrix.
- An eigenvalue of $A$ is a number $\lambda$ such that there exists a non-zero vector $v \in \mathbb{R}^n$ for which $Av = \lambda v$.
- Since $(\lambda Id - A)0 = 0$, if $v$ is an eigenvector of $A$, then $\lambda Id - A$ is not $1 - 1$.
- In linear algebra language, this is expressed by saying $det(\lambda Id - A) = 0$.
- The previous formula expresses a method to find the eigenvalues of a given matrix $A$.
- Eigenvalues and eigenvectors have important applications throughout all of mathematics.

# Preliminaries: Eigenvalues and Eigenvectors.

- Let $A$ be an $n \times n$ matrix.
- An eigenvalue of $A$ is a number $\lambda$ such that there exists a non-zero vector $v \in \mathbb{R}^n$ for which $Av = \lambda v$.
- Since $(\lambda Id - A)0 = 0$, if $v$ is an eigenvector of $A$, then $\lambda Id - A$ is not $1 - 1$.
- In linear algebra language, this is expressed by saying $det(\lambda Id - A) = 0$.
- The previous formula expresses a method to find the eigenvalues of a given matrix $A$.
- Eigenvalues and eigenvectors have important applications throughout all of mathematics.

# Preliminaries: Eigenvalues and Eigenvectors.

- Let $A$ be an $n \times n$ matrix.
- An eigenvalue of $A$ is a number $\lambda$ such that there exists a non-zero vector $v \in \mathbb{R}^n$ for which $Av = \lambda v$.
- Since $(\lambda Id - A)0 = 0$, if $v$ is an eigenvector of $A$, then $\lambda Id - A$ is not $1 - 1$.
- In linear algebra language, this is expressed by saying $det(\lambda Id - A) = 0$.
- The previous formula expresses a method to find the eigenvalues of a given matrix $A$.
- Eigenvalues and eigenvectors have important applications throughout all of mathematics.

## Preliminaries: Eigenvalues and Eigenvectors.

- Let $A$ be an $n \times n$ matrix.
- An eigenvalue of $A$ is a number $\lambda$ such that there exists a non-zero vector $v \in \mathbb{R}^n$ for which $Av = \lambda v$.
- Since $(\lambda Id - A)0 = 0$, if $v$ is an eigenvector of $A$, then $\lambda Id - A$ is not $1-1$.
- In linear algebra language, this is expressed by saying $det(\lambda Id - A) = 0$.
- The previous formula expresses a method to find the eigenvalues of a given matrix $A$.
- Eigenvalues and eigenvectors have important applications throughout all of mathematics.

# Preliminaries: Eigenvalues and Eigenvectors.

- Let $A$ be an $n \times n$ matrix.
- An eigenvalue of $A$ is a number $\lambda$ such that there exists a non-zero vector $v \in \mathbb{R}^n$ for which $Av = \lambda v$.
- Since $(\lambda Id - A)0 = 0$, if $v$ is an eigenvector of $A$, then $\lambda Id - A$ is not $1 - 1$.
- In linear algebra language, this is expressed by saying $det(\lambda Id - A) = 0$.
- The previous formula expresses a method to find the eigenvalues of a given matrix $A$.
- Eigenvalues and eigenvectors have important applications throughout all of mathematics.

# Circulant matrices

- To generate a circulant matrix $C$, start out with any vector $\begin{bmatrix} a & b & c \end{bmatrix}$ and cyclically permute the entries to obtain:

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

- What structural features do you observe?
- Computing the eigenvalues and eigenvectors of a circulant matrix is fun!
- Exercise: find one eigenvector and eigenvalue without any formulas (in other words, just by looking at the above matrix).

# Circulant matrices

- To generate a circulant matrix $C$, start out with any vector $\begin{bmatrix} a & b & c \end{bmatrix}$ and cyclically permute the entries to obtain:

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

- What structural features do you observe?
- Computing the eigenvalues and eigenvectors of a circulant matrix is fun!
- Exercise: find one eigenvector and eigenvalue without any formulas (in other words, just by looking at the above matrix).

# Circulant matrices

- To generate a circulant matrix $C$, start out with any vector $\begin{bmatrix} a & b & c \end{bmatrix}$ and cyclically permute the entries to obtain:

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

- What structural features do you observe?
- Computing the eigenvalues and eigenvectors of a circulant matrix is fun!
- Exercise: find one eigenvector and eigenvalue without any formulas (in other words, just by looking at the above matrix).

# Circulant matrices

- To generate a circulant matrix $C$, start out with any vector $\begin{bmatrix} a & b & c \end{bmatrix}$ and cyclically permute the entries to obtain:

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

- What structural features do you observe?
- Computing the eigenvalues and eigenvectors of a circulant matrix is fun!
- Exercise: find one eigenvector and eigenvalue without any formulas (in other words, just by looking at the above matrix).

# Circulant matrices

- To generate a circulant matrix $C$, start out with any vector $\begin{bmatrix} a & b & c \end{bmatrix}$ and cyclically permute the entries to obtain:

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

- What structural features do you observe?
- Computing the eigenvalues and eigenvectors of a circulant matrix is fun!
- Exercise: find one eigenvector and eigenvalue without any formulas (in other words, just by looking at the above matrix).

# Circulant matrices

- Exercise: verify that $\begin{bmatrix}1 & \omega & \omega^2\end{bmatrix}$ is an eigenvector. What is the corresponding eigenvalue?
- Exercise: verify that $\begin{bmatrix}1 & \overline{\omega} & \overline{\omega}^2\end{bmatrix}$ is an eigenvector. What is the corresponding eigenvalue?
- Now let's move on to higher dimensions.
- Consider:

$$W := \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & 0 & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix}_{n \times n}$$

# Circulant matrices

- Exercise: verify that $\begin{bmatrix} 1 & \omega & \omega^2 \end{bmatrix}$ is an eigenvector. What is the corresponding eigenvalue?
- Exercise: verify that $\begin{bmatrix} 1 & \overline{\omega} & \overline{\omega}^2 \end{bmatrix}$ is an eigenvector. What is the corresponding eigenvalue?
- Now let's move on to higher dimensions.
- Consider:

$$W := \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & 0 & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix}_{n \times n}$$

# Circulant matrices

- Exercise: verify that $\begin{bmatrix} 1 & \omega & \omega^2 \end{bmatrix}$ is an eigenvector. What is the corresponding eigenvalue?
- Exercise: verify that $\begin{bmatrix} 1 & \overline{\omega} & \overline{\omega}^2 \end{bmatrix}$ is an eigenvector. What is the corresponding eigenvalue?
- Now let's move on to higher dimensions.
- Consider:

$$W := \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & 0 & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix}_{n \times n}$$

# Circulant matrices

- Exercise: verify that $\begin{bmatrix}1 & \omega & \omega^2\end{bmatrix}$ is an eigenvector. What is the corresponding eigenvalue?
- Exercise: verify that $\begin{bmatrix}1 & \overline{\omega} & \overline{\omega}^2\end{bmatrix}$ is an eigenvector. What is the corresponding eigenvalue?
- Now let's move on to higher dimensions.
- Consider:

$$W := \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & 0 & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix}_{n\times n}$$

- Exercise: verify that $\begin{bmatrix}1 & \omega & \omega^2\end{bmatrix}$ is an eigenvector. What is the corresponding eigenvalue?
- Exercise: verify that $\begin{bmatrix}1 & \overline{\omega} & \overline{\omega}^2\end{bmatrix}$ is an eigenvector. What is the corresponding eigenvalue?
- Now let's move on to higher dimensions.
- Consider:

$$W := \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & 0 & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix}_{n\times n}$$

# Circulant matrices

- The equation $det(\lambda Id - W) = 0$ is equivalent to $\lambda^n - 1 = 0$.
- Exercise: verify this for $n = 3$.
- Therefore the eigenvalues of $W$ are the $n$th roots of unity.
- Recall that the roots of unity are $\omega^k$ for $k = 0, 1, \ldots, n-1$.
- For each root of unity $\lambda$, $v(\lambda) = \begin{bmatrix} 1 & \lambda & \lambda^2 & \ldots & \lambda^{n-1} \end{bmatrix}$ is a corresponding eigenvector.
- Exercise: check the above statement.

- The equation $det(\lambda Id - W) = 0$ is equivalent to $\lambda^n - 1 = 0$.
- Exercise: verify this for $n = 3$.
- Therefore the eigenvalues of $W$ are the $n$th roots of unity.
- Recall that the roots of unity are $\omega^k$ for $k = 0, 1, \ldots, n-1$.
- For each root of unity $\lambda$, $v(\lambda) = \begin{bmatrix} 1 & \lambda & \lambda^2 & \ldots & \lambda^{n-1} \end{bmatrix}$ is a corresponding eigenvector.
- Exercise: check the above statement.

- The equation $det(\lambda Id - W) = 0$ is equivalent to $\lambda^n - 1 = 0$.
- Exercise: verify this for $n = 3$.
- Therefore the eigenvalues of $W$ are the $n$th roots of unity.
- Recall that the roots of unity are $\omega^k$ for $k = 0, 1, \dots, n-1$.
- For each root of unity $\lambda$, $v(\lambda) = \begin{bmatrix} 1 & \lambda & \lambda^2 & \dots & \lambda^{n-1} \end{bmatrix}$ is a corresponding eigenvector.
- Exercise: check the above statement.

# Circulant matrices

- The equation $det(\lambda Id - W) = 0$ is equivalent to $\lambda^n - 1 = 0$.
- Exercise: verify this for $n = 3$.
- Therefore the eigenvalues of $W$ are the $n$th roots of unity.
- Recall that the roots of unity are $\omega^k$ for $k = 0, 1, \ldots, n-1$.
- For each root of unity $\lambda$, $v(\lambda) = \begin{bmatrix} 1 & \lambda & \lambda^2 & \ldots & \lambda^{n-1} \end{bmatrix}$ is a corresponding eigenvector.
- Exercise: check the above statement.

# Circulant matrices

- The equation $det(\lambda Id - W) = 0$ is equivalent to $\lambda^n - 1 = 0$.
- Exercise: verify this for $n = 3$.
- Therefore the eigenvalues of $W$ are the $n$th roots of unity.
- Recall that the roots of unity are $\omega^k$ for $k = 0, 1, \ldots, n-1$.
- For each root of unity $\lambda$, $v(\lambda) = \begin{bmatrix} 1 & \lambda & \lambda^2 & \ldots & \lambda^{n-1} \end{bmatrix}$ is a corresponding eigenvector.
- Exercise: check the above statement.

# Circulant matrices

- The equation $det(\lambda Id - W) = 0$ is equivalent to $\lambda^n - 1 = 0$.
- Exercise: verify this for $n = 3$.
- Therefore the eigenvalues of $W$ are the $n$th roots of unity.
- Recall that the roots of unity are $\omega^k$ for $k = 0, 1, \ldots, n-1$.
- For each root of unity $\lambda$, $v(\lambda) = \begin{bmatrix} 1 & \lambda & \lambda^2 & \ldots & \lambda^{n-1} \end{bmatrix}$ is a corresponding eigenvector.
- Exercise: check the above statement.

# Circulant matrices

- The equation $det(\lambda Id - W) = 0$ is equivalent to $\lambda^n - 1 = 0$.
- Exercise: verify this for $n = 3$.
- Therefore the eigenvalues of $W$ are the $n$th roots of unity.
- Recall that the roots of unity are $\omega^k$ for $k = 0, 1, \dots, n-1$.
- For each root of unity $\lambda$, $v(\lambda) = \begin{bmatrix} 1 & \lambda & \lambda^2 & \dots & \lambda^{n-1} \end{bmatrix}$ is a corresponding eigenvector.
- Exercise: check the above statement.

# Circulant matrices

- Let $D$ be the diagonal matrix containing $\{\omega^k\}_{k=0}^{n-1}$ along its diagonal. Let $Q$ be the matrix that has the eigenvector of $W$ as columns: $Q := \left[v(1) \quad v(\omega) \quad v(\omega^2) \ldots \quad v(\omega^{n-1})\right]$.
- Then $WQ = QD$, (check this!).
- For a given matrix $A$, the matrix $A^* := \overline{A}^T$ is known as the adjoint of $A$.
- One can check that $Q^{-1} = \frac{1}{n} Q^*$.
- Moreover, $(\frac{1}{\sqrt{n}} Q)^{-1} = \sqrt{n} Q^{-1} = (\frac{1}{\sqrt{n}} Q)^*$.
- Matrices which satisfy $A^{-1} = A^*$ are very special! We call them unitary matrices.
- Therefore $W = (\frac{1}{\sqrt{n}} Q) D (\frac{1}{\sqrt{n}} Q)^*$. This is called a unitary diagonalization of $W$.

# Circulant matrices

- Let $D$ be the diagonal matrix containing $\{\omega^k\}_{k=0}^{n-1}$ along its diagonal. Let $Q$ be the matrix that has the eigenvector of $W$ as columns: $Q := \begin{bmatrix} v(1) & v(\omega) & v(\omega^2) \dots & v(\omega^{n-1}) \end{bmatrix}$.
- Then $WQ = QD$, (check this!).
- For a given matrix $A$, the matrix $A^* := \overline{A}^T$ is known as the adjoint of $A$.
- One can check that $Q^{-1} = \frac{1}{n} Q^*$.
- Moreover, $(\frac{1}{\sqrt{n}} Q)^{-1} = \sqrt{n} Q^{-1} = (\frac{1}{\sqrt{n}} Q)^*$.
- Matrices which satisfy $A^{-1} = A^*$ are very special! We call them unitary matrices.
- Therefore $W = (\frac{1}{\sqrt{n}} Q) D (\frac{1}{\sqrt{n}} Q)^*$. This is called a unitary diagonalization of $W$.

# Circulant matrices

- Let $D$ be the diagonal matrix containing $\{\omega^k\}_{k=0}^{n-1}$ along its diagonal. Let $Q$ be the matrix that has the eigenvector of $W$ as columns: $Q := \left[v(1) \quad v(\omega) \quad v(\omega^2) \ldots \quad v(\omega^{n-1})\right]$.
- Then $WQ = QD$, (check this!).
- For a given matrix $A$, the matrix $A^* := \overline{A}^T$ is known as the adjoint of $A$.
- One can check that $Q^{-1} = \frac{1}{n}Q^*$.
- Moreover, $(\frac{1}{\sqrt{n}}Q)^{-1} = \sqrt{n}Q^{-1} = (\frac{1}{\sqrt{n}}Q)^*$.
- Matrices which satisfy $A^{-1} = A^*$ are very special! We call them unitary matrices.
- Therefore $W = (\frac{1}{\sqrt{n}}Q)D(\frac{1}{\sqrt{n}}Q)^*$. This is called a unitary diagonalization of $W$.

# Circulant matrices

- Let $D$ be the diagonal matrix containing $\{\omega^k\}_{k=0}^{n-1}$ along its diagonal. Let $Q$ be the matrix that has the eigenvector of $W$ as columns: $Q := \begin{bmatrix} v(1) & v(\omega) & v(\omega^2) \dots & v(\omega^{n-1}) \end{bmatrix}$.
- Then $WQ = QD$, (check this!).
- For a given matrix $A$, the matrix $A^* := \overline{A}^T$ is known as the adjoint of $A$.
- One can check that $Q^{-1} = \frac{1}{n} Q^*$.
- Moreover, $(\frac{1}{\sqrt{n}} Q)^{-1} = \sqrt{n} Q^{-1} = (\frac{1}{\sqrt{n}} Q)^*$.
- Matrices which satisfy $A^{-1} = A^*$ are very special! We call them unitary matrices.
- Therefore $W = (\frac{1}{\sqrt{n}} Q) D (\frac{1}{\sqrt{n}} Q)^*$. This is called a unitary diagonalization of $W$.

# Circulant matrices

- Let $D$ be the diagonal matrix containing $\{\omega^k\}_{k=0}^{n-1}$ along its diagonal. Let $Q$ be the matrix that has the eigenvector of $W$ as columns: $Q := \begin{bmatrix} v(1) & v(\omega) & v(\omega^2) \dots & v(\omega^{n-1}) \end{bmatrix}$.
- Then $WQ = QD$, (check this!).
- For a given matrix $A$, the matrix $A^* := \overline{A}^T$ is known as the adjoint of $A$.
- One can check that $Q^{-1} = \frac{1}{n}Q^*$.
- Moreover, $(\frac{1}{\sqrt{n}}Q)^{-1} = \sqrt{n}Q^{-1} = (\frac{1}{\sqrt{n}}Q)^*$.
- Matrices which satisfy $A^{-1} = A^*$ are very special! We call them unitary matrices.
- Therefore $W = (\frac{1}{\sqrt{n}}Q)D(\frac{1}{\sqrt{n}}Q)^*$. This is called a unitary diagonalization of $W$.

- Let $D$ be the diagonal matrix containing $\{\omega^k\}_{k=0}^{n-1}$ along its diagonal. Let $Q$ be the matrix that has the eigenvector of $W$ as columns: $Q := \left[v(1) \quad v(\omega) \quad v(\omega^2) \ldots \quad v(\omega^{n-1})\right]$.
- Then $WQ = QD$, (check this!).
- For a given matrix $A$, the matrix $A^* := \overline{A}^T$ is known as the adjoint of $A$.
- One can check that $Q^{-1} = \frac{1}{n}Q^*$.
- Moreover, $(\frac{1}{\sqrt{n}}Q)^{-1} = \sqrt{n}Q^{-1} = (\frac{1}{\sqrt{n}}Q)^*$.
- Matrices which satisfy $A^{-1} = A^*$ are very special! We call them unitary matrices.
- Therefore $W = (\frac{1}{\sqrt{n}}Q)D(\frac{1}{\sqrt{n}}Q)^*$. This is called a unitary diagonalization of $W$.

# Circulant matrices

- For $n = 3$ verify that

$$aId + bW + cW^2 = \begin{bmatrix} a & b & c \\ c & a & b \\ b & c & a \end{bmatrix}.$$

- In general, the space of circulant matrices is precisely the algebra generated by $W$: namely, the matrices expressible as polynomials $q(W) := a_0 + a_1 W + a_2 W^2 + \ldots + a_{n-1} W^{n-1}$.
- A result from matrix theory states that for a given polynomial $q$, if $Av = \lambda v$, then $q(A)v = q(\lambda)v$.

# Circulant matrices

- For $n = 3$ verify that

$$aId + bW + cW^2 = \begin{bmatrix} a & b & c \\ c & a & b \\ b & c & a \end{bmatrix}.$$

- In general, the space of circulant matrices is precisely the algebra generated by $W$: namely, the matrices expressible as polynomials $q(W) := a_0 + a_1 W + a_2 W^2 + \ldots + a_{n-1} W^{n-1}$.
- A result from matrix theory states that for a given polynomial $q$, if $Av = \lambda v$, then $q(A)v = q(\lambda)v$.

# Circulant matrices

- For $n = 3$ verify that

$$aId + bW + cW^2 = \begin{bmatrix} a & b & c \\ c & a & b \\ b & c & a \end{bmatrix}.$$

- In general, the space of circulant matrices is precisely the algebra generated by $W$: namely, the matrices expressible as polynomials $q(W) := a_0 + a_1 W + a_2 W^2 + \ldots + a_{n-1} W^{n-1}$.
- A result from matrix theory states that for a given polynomial $q$, if $Av = \lambda v$, then $q(A)v = q(\lambda)v$.

# Circulant matrices

- For $n = 3$ verify that

$$aId + bW + cW^2 = \begin{bmatrix} a & b & c \\ c & a & b \\ b & c & a \end{bmatrix}.$$

- In general, the space of circulant matrices is precisely the algebra generated by $W$: namely, the matrices expressible as polynomials $q(W) := a_0 + a_1 W + a_2 W^2 + \ldots + a_{n-1} W^{n-1}$.
- A result from matrix theory states that for a given polynomial $q$, if $Av = \lambda v$, then $q(A)v = q(\lambda)v$.

# Circulant matrices

- Therefore if $C$ is an $n \times n$ circulant matrix, we can use its first row $\begin{bmatrix} a_0 & a_1 & a_2 & \ldots & a_{n-1} \end{bmatrix}$ to define a polynomial $q(t) = a_0 + a_1 t + a_2 t^2 + \ldots + a_{n-1} t^{n-1}$.
- Since $C = q(W)$, the eigenvalues of $C$ are precisely $q(\lambda)$ where $\lambda$ is a root of unity.
- In particular, $C = q(W) = (\frac{1}{\sqrt{n}} Q) q(D) (\frac{1}{\sqrt{n}} Q)^*$.

- Therefore if $C$ is an $n \times n$ circulant matrix, we can use its first row $\begin{bmatrix} a_0 & a_1 & a_2 & \dots & a_{n-1} \end{bmatrix}$ to define a polynomial $q(t) = a_0 + a_1 t + a_2 t^2 + \dots + a_{n-1} t^{n-1}$.
- Since $C = q(W)$, the eigenvalues of $C$ are precisely $q(\lambda)$ where $\lambda$ is a root of unity.
- In particular, $C = q(W) = (\frac{1}{\sqrt{n}} Q) q(D) (\frac{1}{\sqrt{n}} Q)^*$.

# Circulant matrices

- Therefore if $C$ is an $n \times n$ circulant matrix, we can use its first row $\begin{bmatrix} a_0 & a_1 & a_2 & \dots & a_{n-1} \end{bmatrix}$ to define a polynomial $q(t) = a_0 + a_1 t + a_2 t^2 + \dots + a_{n-1} t^{n-1}$.
- Since $C = q(W)$, the eigenvalues of $C$ are precisely $q(\lambda)$ where $\lambda$ is a root of unity.
- In particular, $C = q(W) = (\frac{1}{\sqrt{n}} Q) q(D) (\frac{1}{\sqrt{n}} Q)^*$.

# Circulant matrices

- Therefore if $C$ is an $n \times n$ circulant matrix, we can use its first row $\begin{bmatrix} a_0 & a_1 & a_2 & \dots & a_{n-1} \end{bmatrix}$ to define a polynomial $q(t) = a_0 + a_1 t + a_2 t^2 + \ldots + a_{n-1} t^{n-1}$.
- Since $C = q(W)$, the eigenvalues of $C$ are precisely $q(\lambda)$ where $\lambda$ is a root of unity.
- In particular, $C = q(W) = (\frac{1}{\sqrt{n}} Q) q(D) (\frac{1}{\sqrt{n}} Q)^*$.

# Circulant matrices

- Example: let

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

- Since the dimension is $n = 4$, the $n$th roots of unity are $1, -1, i, -i$. The polynomial $q(t)$ can be constructed from the first row of $C$ as $q(t) = 1 + 2t + t^2 + 3t^3$.
- Thus the eigenvalues of $C$ are simply $q(1) = 7$, $q(-1) = -3$, $q(-i) = -i$, and $q(-i) = i$.
- The corresponding eigenvectors are $v(1) = (1, 1, 1, 1)$, $v(-1) = (-1, -1, 1, -1)$, $v(i) = (1, i, -1, -i)$, and $v(-i) = (1, -i, -1, i)$.

# Circulant matrices

- Example: let

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

- Since the dimension is $n = 4$, the $n$th roots of unity are $1, -1, i, -i$. The polynomial $q(t)$ can be constructed from the first row of $C$ as $q(t) = 1 + 2t + t^2 + 3t^3$.
- Thus the eigenvalues of $C$ are simply $q(1) = 7$, $q(-1) = -3$, $q(-i) = -i$, and $q(-i) = i$.
- The corresponding eigenvectors are $v(1) = (1, 1, 1, 1)$, $v(-1) = (-1, -1, 1, -1)$, $v(i) = (1, i, -1, -i)$, and $v(-i) = (1, -i, -1, i)$.

# Circulant matrices

- Example: let
$$C = \begin{bmatrix} 1 & 2 & 1 & 3 \\ 3 & 1 & 2 & 1 \\ 1 & 3 & 1 & 2 \\ 2 & 1 & 3 & 1 \end{bmatrix}.$$
- Since the dimension is $n = 4$, the $n$th roots of unity are $1, -1, i, -i$. The polynomial $q(t)$ can be constructed from the first row of $C$ as $q(t) = 1 + 2t + t^2 + 3t^3$.
- Thus the eigenvalues of $C$ are simply $q(1) = 7$, $q(-1) = -3$, $q(-i) = -i$, and $q(-i) = i$.
- The corresponding eigenvectors are $v(1) = (1, 1, 1, 1)$, $v(-1) = (-1, -1, 1, -1)$, $v(i) = (1, i, -1, -i)$, and $v(-i) = (1, -i, -1, i)$.

# Circulant matrices

- Example: let
$$C = \begin{bmatrix} 1 & 2 & 1 & 3 \\ 3 & 1 & 2 & 1 \\ 1 & 3 & 1 & 2 \\ 2 & 1 & 3 & 1 \end{bmatrix}.$$
- Since the dimension is $n = 4$, the $n$th roots of unity are $1, -1, i, -i$. The polynomial $q(t)$ can be constructed from the first row of $C$ as $q(t) = 1 + 2t + t^2 + 3t^3$.
- Thus the eigenvalues of $C$ are simply $q(1) = 7$, $q(-1) = -3$, $q(-i) = -i$, and $q(-i) = i$.
- The corresponding eigenvectors are $v(1) = (1, 1, 1, 1)$, $v(-1) = (-1, -1, 1, -1)$, $v(i) = (1, i, -1, -i)$, and $v(-i) = (1, -i, -1, i)$.

- Example: let

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

- Since the dimension is $n = 4$, the $n$th roots of unity are $1, -1, i, -i$. The polynomial $q(t)$ can be constructed from the first row of $C$ as $q(t) = 1 + 2t + t^2 + 3t^3$.
- Thus the eigenvalues of $C$ are simply $q(1) = 7$, $q(-1) = -3$, $q(-i) = -i$, and $q(-i) = i$.
- The corresponding eigenvectors are $v(1) = (1, 1, 1, 1)$, $v(-1) = (-1, -1, 1, -1)$, $v(i) = (1, i, -1, -i)$, and $v(-i) = (1, -i, -1, i)$.

# Polynomial equations

- Consider the quadratic polynomial $p(t) = t^2 + \alpha t + \beta$.
- It's fun to find a formula for its roots using circulant matrix theory.
- Consider a general $2 \times 2$ circulant

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

- The characteristic polynomial of $C$ is $\det(\lambda Id - C) = \det\left(\begin{bmatrix} \lambda - a & -b \\ -b & \lambda - a \end{bmatrix}\right) = \lambda^2 - 2a\lambda + a^2 - b^2.$

# Polynomial equations

- Consider the quadratic polynomial $p(t) = t^2 + \alpha t + \beta$.
- It's fun to find a formula for its roots using circulant matrix theory.
- Consider a general $2 \times 2$ circulant

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

- The characteristic polynomial of $C$ is

$$\det(\lambda Id - C) = \det\left(\begin{bmatrix} \lambda - a & -b \\ -b & \lambda - a \end{bmatrix}\right) = \lambda^2 - 2a\lambda + a^2 - b^2.$$

# Polynomial equations

- Consider the quadratic polynomial $p(t) = t^2 + \alpha t + \beta$.
- It's fun to find a formula for its roots using circulant matrix theory.
- Consider a general $2 \times 2$ circulant

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

- The characteristic polynomial of $C$ is

$$\det(\lambda Id - C) = \det\left(\begin{bmatrix} \lambda - a & -b \\ -b & \lambda - a \end{bmatrix}\right) = \lambda^2 - 2a\lambda + a^2 - b^2.$$

# Polynomial equations

- Consider the quadratic polynomial $p(t) = t^2 + \alpha t + \beta$.
- It's fun to find a formula for its roots using circulant matrix theory.
- Consider a general $2 \times 2$ circulant

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

- The characteristic polynomial of $C$ is

$$\det(\lambda Id - C) = \det\left(\begin{bmatrix} \lambda - a & -b \\ -b & \lambda - a \end{bmatrix}\right) = \lambda^2 - 2a\lambda + a^2 - b^2.$$

# Polynomial equations

- Consider the quadratic polynomial $p(t) = t^2 + \alpha t + \beta$.
- It's fun to find a formula for its roots using circulant matrix theory.
- Consider a general $2 \times 2$ circulant

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

- The characteristic polynomial of $C$ is $\det(\lambda Id - C) = \det\left(\begin{bmatrix} \lambda - a & -b \\ -b & \lambda - a \end{bmatrix}\right) = \lambda^2 - 2a\lambda + a^2 - b^2.$

# Polynomial equations

- Our task is to find $a$ and $b$ so that the characteristic polynomial of $C$ is $p$.
- In other words we must solve $-2a = \alpha$ and $a^2 - b^2 = \beta$.
- Therefore $a = \frac{-\alpha}{2}$ and $b = \pm\sqrt{\frac{\alpha^2}{4} - \beta}$.
- Thus we may choose

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

# Polynomial equations

- Our task is to find $a$ and $b$ so that the characteristic polynomial of $C$ is $p$.
- In other words we must solve $-2a = \alpha$ and $a^2 - b^2 = \beta$.
- Therefore $a = \frac{-\alpha}{2}$ and $b = \pm\sqrt{\frac{\alpha^2}{4} - \beta}$.
- Thus we may choose

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

# Polynomial equations

- Our task is to find $a$ and $b$ so that the characteristic polynomial of $C$ is $p$.
- In other words we must solve $-2a = \alpha$ and $a^2 - b^2 = \beta$.
- Therefore $a = \frac{-\alpha}{2}$ and $b = \pm\sqrt{\frac{\alpha^2}{4} - \beta}$.
- Thus we may choose

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

# Polynomial equations

- Our task is to find $a$ and $b$ so that the characteristic polynomial of $C$ is $p$.
- In other words we must solve $-2a = \alpha$ and $a^2 - b^2 = \beta$.
- Therefore $a = \frac{-\alpha}{2}$ and $b = \pm\sqrt{\frac{\alpha^2}{4} - \beta}$.
- Thus we may choose

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

- Our task is to find $a$ and $b$ so that the characteristic polynomial of $C$ is $p$.
- In other words we must solve $-2a = \alpha$ and $a^2 - b^2 = \beta$.
- Therefore $a = \frac{-\alpha}{2}$ and $b = \pm\sqrt{\frac{\alpha^2}{4} - \beta}$.
- Thus we may choose

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

# Polynomial equations

- In particular $q(t) = \frac{-\alpha}{2} + t\sqrt{\frac{\alpha^2}{4} - \beta} = \frac{-\alpha + t\sqrt{\alpha^2 - 4\beta}}{2}$.
- The roots of $p$ are the eigenvalues of $C$ given by plugging in the two roots of unity into $q$: $q(-1) = \frac{-\alpha - \sqrt{\alpha^2 - 4\beta}}{2}$ and $q(1) = \frac{-\alpha + \sqrt{\alpha^2 - 4\beta}}{2}$.
- But this is just the quadratic formula which was discovered more than 4000 years ago.

# Polynomial equations

- In particular $q(t) = \frac{-\alpha}{2} + t\sqrt{\frac{\alpha^2}{4} - \beta} = \frac{-\alpha + t\sqrt{\alpha^2 - 4\beta}}{2}$.
- The roots of $p$ are the eigenvalues of $C$ given by plugging in the two roots of unity into $q$: $q(-1) = \frac{-\alpha - \sqrt{\alpha^2 - 4\beta}}{2}$ and $q(1) = \frac{-\alpha + \sqrt{\alpha^2 - 4\beta}}{2}$.
- But this is just the quadratic formula which was discovered more than 4000 years ago.

# Polynomial equations

- In particular $q(t) = \frac{-\alpha}{2} + t\sqrt{\frac{\alpha^2}{4} - \beta} = \frac{-\alpha + t\sqrt{\alpha^2 - 4\beta}}{2}$.
- The roots of $p$ are the eigenvalues of $C$ given by plugging in the two roots of unity into $q$: $q(-1) = \frac{-\alpha - \sqrt{\alpha^2 - 4\beta}}{2}$ and $q(1) = \frac{-\alpha + \sqrt{\alpha^2 - 4\beta}}{2}$.
- But this is just the quadratic formula which was discovered more than 4000 years ago.

# Polynomial equations

- In particular $q(t) = \frac{-\alpha}{2} + t\sqrt{\frac{\alpha^2}{4} - \beta} = \frac{-\alpha + t\sqrt{\alpha^2 - 4\beta}}{2}$.
- The roots of $p$ are the eigenvalues of $C$ given by plugging in the two roots of unity into $q$: $q(-1) = \frac{-\alpha - \sqrt{\alpha^2 - 4\beta}}{2}$ and $q(1) = \frac{-\alpha + \sqrt{\alpha^2 - 4\beta}}{2}$.
- But this is just the quadratic formula which was discovered more than 4000 years ago.

# Polynomial equations

- The cool part is that we can now easily apply the circulant matrix strategy to solve cubic and quartic polynomial equations and re-derive the famous Cardano formulas discovered in 1545. This will be your task: see the worksheet.
- Mathematicians such as Euler, Bezout, Malfatti, Lagrange, and others struggled to find formulas for the solutions of higher degree polynomials. Ruffini (1799) and Abel (1826) showed that the solution of the general quintic equation cannot be written as a finite formula in terms of the four arithmetic operations and the taking of roots.
- By 1832, Galois developed a theory to describe when a polynomial equation is solvable.

# Polynomial equations

- The cool part is that we can now easily apply the circulant matrix strategy to solve cubic and quartic polynomial equations and re-derive the famous Cardano formulas discovered in 1545. This will be your task: see the worksheet.
- Mathematicians such as Euler, Bezout, Malfatti, Lagrange, and others struggled to find formulas for the solutions of higher degree polynomials. Ruffini (1799) and Abel (1826) showed that the solution of the general quintic equation cannot be written as a finite formula in terms of the four arithmetic operations and the taking of roots.
- By 1832, Galois developed a theory to describe when a polynomial equation is solvable.

- The cool part is that we can now easily apply the circulant matrix strategy to solve cubic and quartic polynomial equations and re-derive the famous Cardano formulas discovered in 1545. This will be your task: see the worksheet.
- Mathematicians such as Euler, Bezout, Malfatti, Lagrange, and others struggled to find formulas for the solutions of higher degree polynomials. Ruffini (1799) and Abel (1826) showed that the solution of the general quintic equation cannot be written as a finite formula in terms of the four arithmetic operations and the taking of roots.
- By 1832, Galois developed a theory to describe when a polynomial equation is solvable.

# Polynomial equations

- The cool part is that we can now easily apply the circulant matrix strategy to solve cubic and quartic polynomial equations and re-derive the famous Cardano formulas discovered in 1545. This will be your task: see the worksheet.
- Mathematicians such as Euler, Bezout, Malfatti, Lagrange, and others struggled to find formulas for the solutions of higher degree polynomials. Ruffini (1799) and Abel (1826) showed that the solution of the general quintic equation cannot be written as a finite formula in terms of the four arithmetic operations and the taking of roots.
- By 1832, Galois developed a theory to describe when a polynomial equation is solvable.

- The connection between circulant matrices and polynomial equations was developed by Kalman and White in their 2001 paper "Polynomial equations and circulant matrices."
- There are many other neat applications of circulant matrix theory. For instance, it turns out that one may apply this theory to prove a quantitative version of the polygonal isoperimetric inequality. This is joint work with my friend Levon Nurbekyan – our paper will be available very soon.

- The connection between circulant matrices and polynomial equations was developed by Kalman and White in their 2001 paper "Polynomial equations and circulant matrices."
- There are many other neat applications of circulant matrix theory. For instance, it turns out that one may apply this theory to prove a quantitative version of the polygonal isoperimetric inequality. This is joint work with my friend Levon Nurbekyan – our paper will be available very soon.

- The connection between circulant matrices and polynomial equations was developed by Kalman and White in their 2001 paper "Polynomial equations and circulant matrices."
- There are many other neat applications of circulant matrix theory. For instance, it turns out that one may apply this theory to prove a quantitative version of the polygonal isoperimetric inequality. This is joint work with my friend Levon Nurbekyan – our paper will be available very soon.

# For Further Reading


E. Indrei and L. Nurbekyan
A circulant matrix theory approach to quantitative polygonal isoperimetric inequalities.
Preprint, 2013.

D. Kalman and J.E. White
Polynomial equations and circulant matrices.
*Amer. Math. Monthly*, November 2001.