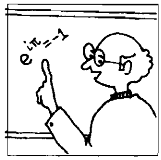

In this section of *Resonance*, we invite readers to pose questions likely to be raised in a classroom situation. We may suggest strategies for dealing with them, or invite responses, or both. "Classroom" is equally a forum for raising broader issues and sharing personal experiences and viewpoints on matters related to teaching and learning science.

A John Wilson
Department of Mathematics
Coimbatore Institute of Technology
Coimbatore 641 014
Tamil Nadu, India.
Email
johnwilsonpr@yahoo.com

Inverting Matrices Constructed from Roots of Unity

Imagine a situation where one has a function $f(x)$ which is known to be equal to (or approximable by) a polynomial function $c_0 + c_1x + c_2x^2 + \quad + c_{n-1}x^{n-1}$ but one does not know what the coefficients $c_0, \quad , c_{n-1}$ (of this interpolating polynomial) are. If one could somehow find the values taken by f at some n distinct points $a_0, a_1, \quad , a_{n-1}$, one can determine the values of the c_i's from the usual method of solving a system of linear equations. Indeed, let $f(a_i) = b_i$ for $i = 0, 1, \quad , n-1$. Then,

$$c_0 + c_1a_i + c_2a_i^2 + \quad + c_{n-1}a_i^{n-1} = b_i \ \forall\ i \leq n-1.$$

One can rephrase this as a matrix equation

$$\begin{pmatrix} 1 & a_0 & a_0^2 & & a_0^{n-1} \\ 1 & a_1 & a_1^2 & & a_1^{n-1} \\ & \ddots & \ddots & \ddots & \vdots \\ 1 & a_{n-1} & a_{n-1}^2 & & a_{n-1}^{n-1} \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ \\ c_{n-1} \end{pmatrix} = \begin{pmatrix} b_0 \\ b_1 \\ \\ b_{n-1} \end{pmatrix}$$

Let us write this matrix equation as $\mathbf{Ac} = \mathbf{b}$. Therefore, if one could find the inverse of the matrix A, then we would determine the c_i's as $\mathbf{A^{-1}b} = \mathbf{c}$.

Keywords
Roots of unity, symmetric matrix, unitary matrix.

This is one situation when one naturally comes across a matrix A of the above form which one wants to invert. In general, there is no easy way but in this note we look at such a matrix A where the a_i's are nth roots of unity and show that it is indeed very easy to compute its inverse.

A matrix of the form considered here is easy to invert since sums of powers of roots of unity are quite often zero.

Let ζ denote a primitive nth root of unity. This means $\zeta^n = 1$ but $\zeta^m \neq 1$ for $0 < m < n$. So, ζ is either $e^{2i\pi/n}$ or its kth power for some k relatively prime to n.

Consider the matrix

$$\begin{pmatrix} 1 & 1 & 1 & & 1 \\ 1 & \zeta & \zeta^2 & & \zeta^{n-1} \\ 1 & \zeta^2 & \zeta^4 & & \zeta^{2(n-1)} \\ & \ddots & \ddots & \ddots & \ddots \\ 1 & \zeta^{n-1} & \zeta^{2(n-1)} & & \zeta^{(n-1)^2} \end{pmatrix}$$

The main idea here is that sums of powers of roots of unity are quite often zero. Indeed, recall something all of us learnt quite early in school – the sum of a finite geometric progression (G.P.) of numbers $a, ar, ar^2, \quad, ar^{n-1}$ is $\frac{a(r^n-1)}{r-1}$ if $r \neq 1$, and, if $r = 1$, the sum is clearly na. As this is valid for complex a, r also, one could take for r, a primitive nth root of unity. Obviously, then the sum is zero.

In a nutshell, if we look at the product of the above matrix with a matrix defined analogously by replacing ζ by some power of ζ, most of the entries turn out to be zero in view of this simple fact about the G.P. In fact, upto permuting the rows, the product matrix is a diagonal matrix.

Thus, it makes sense to consider along with the above matrix $M(\zeta)$, its sister matrices $M(\zeta^r)$ also. For any r relatively prime to n, the number ζ^r is also a primitive nth root of unity and let us denote by $M(\zeta^r)$ the matrix analogous to $M(\zeta)$ where ζ is replaced by ζ^r That is,

$$M(\zeta^r) = \begin{pmatrix} 1 & 1 & 1 & & 1 \\ 1 & \zeta^r & \zeta^{2r} & & \zeta^{(n-1)r} \\ 1 & \zeta^{2r} & \zeta^{4r} & & \zeta^{2(n-1)r} \\ \ddots & \ddots & \ddots & \ddots & \ddots \\ 1 & \zeta^{(n-1)r} & \zeta^{2(n-1)r} & & \zeta^{(n-1)^2 r} \end{pmatrix}$$

We first observe :

Observation

$M(\zeta^r)$ is a symmetric matrix for each r. Indeed, the (i,j)th entry is $\zeta^{r(i-1)(j-1)}$. The rows of the matrix $M(\zeta^r)$ are obtained by permuting those of $M(\zeta)$. In fact, the permutation is that which associates to each $i \leq n$, the residue of ri modulo n. In particular, the matrix $M(\zeta^r)$ has determinant $\pm$ det $M(\zeta)$.

For integers r, s, both relatively prime to n, the product $M(\zeta^s)M(\zeta^r)$ can easily be computed as follows.

Theorem

$(M(\zeta^s)M(\zeta^r))_{ij} = n$ or 0 according as to whether n divides $s(i-1)+r(j-1)$ or not. In particular, the product matrix has only one nonzero entry in each row and each column and this entry is n. As a further particular case, $M(\zeta)M(\zeta^{n-1})$ is the scalar matrix nI

Proof. If a_{ij} and b_{ij} are the (i,j)th entries of $M(\zeta^s)$ and $M(\zeta^r)$ respectively, then clearly, $a_{ij} = \zeta^{s(i-1)(j-1)}$ and $b_{ij} = \zeta^{r(i-1)(j-1)}$. The (i,j)th entry of $M(\zeta^s)(M(\zeta^r)$ is

$$\sum_{k=1}^{n} a_{ik}b_{kj} = \sum_{k=1}^{n} \zeta^{(k-1)(s(i-1)+r(j-1))} = \sum_{k=0}^{n-1} \zeta^{k(s(i-1)+r(j-1))}.$$

Summing a finite geometric progression, one sees easily that $\sum_{k=0}^{n-1} \zeta^{kl} = n$ or 0 according as to whether n divides l or not.

Thus, we have $(M(\zeta^s)M(\zeta^r))_{ij} = n$ or 0 according as to whether n divides $s(i-1) + r(j-1)$ or not.

Therefore, for each $j \leq n$, there is a unique i such that the (i,j)th entry is nonzero; it is $i = 1 + s^{-1}r(1-j)$ modulo n. In other words, the product matrix has only one nonzero entry in each row and each column and this entry is n. In particular, $M(\zeta)M(\zeta^{n-1})$ is the scalar matrix nI.

Corollary

$M(\zeta)^{-1} = \frac{1}{n}M(\zeta^{n-1})$. Therefore, the matrix $\frac{1}{\sqrt{n}}M(\zeta)$ is a unitary matrix.

Proof. The first statement is immediate from the theorem. So, the inverse of $\frac{1}{\sqrt{n}}M(\zeta)$ is $\frac{1}{\sqrt{n}}M(\zeta^{n-1})$. But, since $\zeta^{n-1} = \bar{\zeta}$, the above matrix is simply the conjugate transpose. Thus, the matrix $\frac{1}{\sqrt{n}}M(\zeta)$ is a unitary matrix.

Remarks and Examples

From the unitarity of $\frac{1}{\sqrt{n}}M(\zeta)$, it is clear that the determinant of the matrix $M(\zeta)$ is $\pm n^{n/2}$ or $\pm i n^{n/2}$. The sign depends on the choice of ζ. Also, as we will show below, the value of the determinant is real or imaginary according as to whether n is $1, 2 \bmod 4$ or as to whether n is $0, 3 \bmod 4$. We first give some examples.

Examples

(i) $n = 2,\ \zeta = -1$.

Then, note that det $M(\zeta) = -2$ and that $\frac{1}{\sqrt{2}}M(\zeta) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and its inverse is itself.

(ii) $n = 3,\ \zeta = e^{2i\pi/3} = \frac{-1+i\sqrt{3}}{2}$.

Then,

$M(\zeta) = \begin{pmatrix} 1 & 1 & 1 \\ 1 & e^{2i\pi/3} & e^{4i\pi/3} \\ 1 & e^{4i\pi/3} & e^{2i\pi/3} \end{pmatrix}$ which has determinant

$-3\sqrt{3}i$. The inverse of $\frac{1}{\sqrt{3}}M(e^{2i\pi/3})$ is $\frac{1}{\sqrt{3}}M(e^{-2i\pi/3}) =$

$$\frac{1}{\sqrt{3}}\begin{pmatrix} 1 & 1 & 1 \\ 1 & e^{-2i\pi/3} & e^{-4i\pi/3} \\ 1 & e^{-4i\pi/3} & e^{-2i\pi/3} \end{pmatrix}$$

(iii) $n = 4,\ \zeta = i$.

The inverse of $\frac{1}{2}M(i)$ is $\frac{1}{2}M(-i)$.

A Method to Find det $(M(\zeta))^2$ Directly:

Here is another way to find the square of the determinant of $M(\zeta)$ (which is, of course, the same as the square of the determinant of $M(\zeta^r)$ for each r relatively prime to n).

The matrices of the form $M(\zeta)$ are special cases of the Vandermonde matrices. For distinct complex numbers $\alpha_1, \quad, \alpha_n$, the matrix

$$V = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & & \alpha_2^{n-1} \\ \ddots & \ddots & \ddots & \ddots & \ddots \\ 1 & \alpha_n & \alpha_n^2 & & \alpha_n^{n-1} \end{pmatrix}$$

has determinant $\prod_{i>j\geq 1}(\alpha_i - \alpha_j)$. This is easily proved by induction on n.

Using this, we get det $M(\zeta) = \prod_{n>i>j\geq 0}(\zeta^i - \zeta^j)$.

Putting $f(x) = x^n - 1 = \prod_{r=0}^{n-1}(x - \zeta^r)$, we have two expressions for $f'(\zeta^s)$ from the two sides of the above product, as follows.

$$f'(\zeta^s) = n\zeta^{-s} = \prod_{r:r\neq s}(\zeta^s - \zeta^r).$$

Thus,

$$det\ M(\zeta)^2 = (-1)^{\binom{n}{2}} \prod_{n>i\neq j\geq 0}(\zeta^i - \zeta^j) =$$

$$(-1)^{\binom{n}{2}} \prod_{r=0}^{n-1} f'(\zeta^r) = (-1)^{\binom{n}{2}} n^n \zeta^{n(n-1)/2}$$

Now, $\zeta^{n(n-1)/2} = (\zeta^n)^{(n-1)/2} = 1$ when n is odd, and $\zeta^{n(n-1)/2} = (\zeta^{n/2})^{n-1} = (-1)^{n-1} = -1$ when n is even.

Therefore, $\det M(\zeta)^2 = (-1)^{\binom{n}{2}} n^n$ or $-(-1)^{\binom{n}{2}} n^n$ according as to whether n is odd or even. This is $n^{n/2}$ when $n \equiv 1, 2 \mod 4$ and $-n^{n/2}$ when $n \equiv 0, 3 \mod 4$. Consequently, $\det M(\zeta) = \pm n^{n/2}$ when $n \equiv 1, 2 \mod 4$ and $\det M(\zeta) = \pm i n^{n/2}$ when $n \equiv 0, 3 \mod 4$.

Analogue for Cyclic Groups mod Primes:

The above discussion carries over to give us the following analogue. If p is a prime number, consider the group $\{1, 2, \quad, p-1\}$ of integers with the operation of multiplication modulo p. This is a cyclic group of order $p-1$. If ζ is a generator of this group, then once again, it can be seen that $\sum_{k=1}^{p-1} \zeta^{kl}$ equals either $p-1$ or 0 according as to whether l is a multiple of $p-1$ or not. This is seen simply by multiplying the above sum S by ζ^l and observing that $\zeta^l S = S$. Thus, exactly as before, one obtains :

If p is a prime number, consider the group {1,2, ..., p – 1} of integers with the operation of multiplication modulo p. If ζ is a generator of this group, then it can be seen that $\sum_{k=1}^{p-1} \zeta^{kl}$ equals either $p-1$ or 0 according as to whether l is a multiple of $p-1$ or not.

Theorem

Let $M(\zeta)$ be the $(p-1) \times (p-1)$ matrix whose entries are integers mod p, defined as follows.

$$M(\zeta) = \begin{pmatrix} 1 & 1 & 1 & & 1 \\ 1 & \zeta & \zeta^2 & & \zeta^{p-2} \\ 1 & \zeta^2 & \zeta^4 & & \zeta^{2(p-2)} \\ & & \ddots & \ddots & \ddots \\ 1 & \zeta^{p-2} & \zeta^{2(p-2)} & & \zeta^{(p-2)^2} \end{pmatrix}$$

Then, $M(\zeta)M(\zeta^{-1})$ is the scalar matrix $(p-1)I = -I$ Thus, $M(\zeta)^{-1} = -M(\zeta^{-1})$.

Indeed, the whole argument goes through for any prime power q where ζ is a generator of the cyclic group of all nonzero elements in the finite field with q elements.

Examples

(i) $p = 3,\ \zeta = 2$.

Then, $M(\zeta) = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ has inverse $-M(\zeta^{-1}) = -M(\zeta)$.

(ii) $p = 5,\ \zeta = 2$.

Then, $M(2) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 3 \\ 1 & 4 & 1 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$ has inverse $-M(\zeta^{-1}) =$ $M(3)$,

where $M(3) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 3 & 4 & 2 \\ 1 & 4 & 1 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$

(iii) $p = 7,\ \zeta = 3$.

Then, $M(3) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 2 & 6 & 4 & 5 \\ 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 4 & 2 & 1 & 4 & 2 \\ 1 & 5 & 4 & 6 & 2 & 3 \end{pmatrix}$ has inverse

$-M(3^{-1}) = -M(5)$,

where $M(5) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 5 & 4 & 6 & 2 & 3 \\ 1 & 4 & 2 & 1 & 4 & 2 \\ 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 3 & 2 & 6 & 4 & 5 \end{pmatrix}$