On the Eigenvectors of Schur's Matrix

PATRICK MORTON*

Department of Mathematics, University of Michigan, Ann Arbor, Michigan 48109

Communicated by D. J. Lewis
Received November 1, 1978

A basis of eigenvectors is given for the matrix \( \mathcal{U} = (e^{2\pi i mn/q}) \), \((1 \leq m, n < q)\).

The eigenvectors arise from the characters on the reduced residue class group \((\text{mod } q)\).

In this note we exhibit a simple basis of eigenvectors for the matrix

\[ \mathcal{U} = (e^{2\pi i mn/q}) \quad (1 \leq m, n < q), \]

where \( q \) is a positive integer. The eigenvalues of \( \mathcal{U} \) are well known. They are contained among the numbers \( \frac{\sqrt{q}}{4^a} \) for \( 0 \leq a \leq 3 \) (see [1]), a fact which follows from the observation that \( \mathcal{U}^4 = q^2 I \). Schur [3] used these eigenvalues to evaluate the familiar Gaussian sum

\[ S = \sum_{n=1}^{q} e^{2\pi i n^2/q}, \]

which is the trace of the matrix \( \mathcal{U} \).

The eigenvectors we give arise from the characters of the reduced residue class group modulo \( q \). We begin by recalling a few well-known facts about characters; these can be found in Hasse [2, Sects. 13, 20].

Let \( \chi \) be a character modulo \( q \). The least positive divisor \( f = f(\chi) \) of \( q \) with the property that

\[ \chi(n) = 1 \quad \text{for every } n \equiv 1 \pmod{f} \text{ for which } (n, q) = 1, \]

is called the conductor of \( \chi \). The character \( \chi \) can be uniquely defined on the integers \( m \) relatively prime to \( f \) if one sets

\[ \chi(m) = \chi(n), \quad \text{where } m \equiv n \pmod{f} \text{ and } (n, q) = 1. \]

* The author was a National Science Foundation Predoctoral Fellow at the time this article was written. The author's present address is: Department of Mathematics, California Institute of Technology, Pasadena, California 91125.

0022-314X/80/010122-06$02.00/0
Copyright © 1980 by Academic Press, Inc.
All rights of reproduction in any form reserved.
With this definition \( \chi \) becomes a character modulo \( f \). In this note we always consider \( \chi \) defined modulo its conductor, and we set

\[
\chi(n) = 0 \quad \text{if} \quad (n, f(\chi)) > 1.
\]

We shall also need the main properties of the Gaussian sum

\[
\tau(\chi) = \sum_{r=1}^{f} \chi(r) e^{2\pi ir/f}
\]

(2)

associated with \( \chi \). We have that

\[
\tau(\chi) \tau(\bar{x}) = \chi(-1) f(\chi),
\]

(3)

and

\[
\sum_{r=1}^{f} \chi(r) e^{2\pi iar/f} = \overline{\chi(a)} \tau(\chi), \quad \text{for any integer } a.
\]

(4)

Finally, we recall the orthogonality property

\[
\sum_{n=1}^{q} \chi(n) \overline{\psi(n)} = \begin{cases} 0 & \text{if } \chi \neq \psi, \\ \phi(q) & \text{if } \chi = \psi, \end{cases}
\]

(5)

where \( \chi \) and \( \psi \) are any characters (mod \( q \)) and \( \phi \) is the Euler \( \phi \)-function.

We now define a \( q \)-dimensional vector \( X_d \) for every character \( \chi \) and every divisor \( d \) of \( q/f(\chi) \). Let the \( n \)th component of \( X_d \) be

\[
X_d(n) = \begin{cases} \chi(n/d) & \text{if } d \mid n, \\ 0 & \text{if } d \nmid n, \end{cases} \quad \text{for } 1 \leq n \leq q.
\]

(6)

For each character \( \chi \) there are \( d(q/f) \) such vectors, where \( d(n) \) is the number of divisors of \( n \). If \( p(f) \) is the number of characters with conductor \( f \), we see that there are in all

\[
\sum_{f \mid q} p(f) d(q/f) = \sum_{d \mid q} \sum_{f \mid q/d} p(f)
\]

such vectors. Since there are exactly \( \phi(q/d) \) characters (mod \( q/d \)), and since every character with conductor dividing \( q/d \) gives rise to a character (mod \( q/d \)), it follows that the total number of vectors is equal to

\[
\sum_{d \mid q} \phi(q/d) = q.
\]

We now prove the following
Lemma. The $q$ vectors $X_d$ are independent.

Proof. Assume that

$$\sum_x \sum_{d|q/f(x)} c_{x,d} X_d = 0,$$

where the first sum ranges over all the characters (mod $q$). From (6) we then have that

$$\sum_x \sum_{d|q/f(x)} c_{x,d} \chi(n/d) = 0 \quad \text{for} \quad 1 \leq n \leq q. \quad (7)$$

If $n$ is relatively prime to $q$, then (7) reduces to

$$\sum_x c_{x,1} \chi(n) = 0. \quad (8)$$

We now multiply through in (8) by $\psi(n)$, where $\psi$ is any character (mod $q$), and we sum over the reduced residues (mod $q$). By (5) this gives

$$0 = \sum_x c_{x,1} \sum_{(n,d)=1} \chi(n) \psi(n) = \phi(q) c_{x,1}$$

Hence $c_{x,1} = 0$ for every $\chi$.

Now let $d_1$ be any divisor of $q$ and assume that $c_{x,d} = 0$ for all the divisors $d$ of $q$ which are less than $d_1$. Let $m$ be any integer satisfying

$$1 \leq m \leq q/d_1 \quad \text{and} \quad (m,q/d_1) = 1. \quad (9)$$

If we set $n = md_1$ and note $(n,q) = d_1$, then by (7) and the inductive assumption we have

$$\sum_x c_{x,d_1} \chi(m) = 0. \quad (10)$$

This sum is over all the characters which are defined modulo $q/d_1$. If we multiply through in (10) by $\psi(m)$, where $\psi$ is any character (mod $q/d_1$), and sum over the integers $m$ in (9), then we find from (5) as before that $c_{x,d_1} = 0$ for every $\chi$ with $f(\chi) \mid q/d_1$.

It now follows by induction that $c_{x,d} = 0$ for all $\chi$ and $d$, and this implies the assertion of the lemma.

In order to give a basis for the eigenvectors of $\mathcal{A}$ we first compute the vectors $\mathcal{A}X_d$. From (1) and (6) we see that the $m$th component of $\mathcal{A}X_d$ is
EIGENVECTORS OF SCHUR'S MATRIX

\[ \sum_{n=1}^{q} e^{i\pi nmq/n} \chi(n/d) = \sum_{n=1}^{q/d} e \left( \frac{mn}{q/d} \right) \chi(n) \quad (e(\theta) = e^{2\pi i\theta}) \]

\[ = \sum_{r=1}^{q/d} \chi(r) \sum_{k=0}^{q/fd-1} e \left( \frac{mr + kf}{q/d} \right) \]

\[ = \sum_{r=1}^{q/fd} \chi(r) e \left( \frac{mr}{q/d} \right) \sum_{k=0}^{q/fd-1} e \left( \frac{mk}{q/fd} \right) \]

\[ = 0, \quad \text{if} \quad q/fd \not\equiv m \]

\[ = \frac{q}{fd} \sum_{r=1}^{f} \chi(r) e \left( \frac{r}{f} \frac{mdf}{q} \right), \quad \text{if} \quad q/fd \mid m. \] (11)

By (4) the last expression is equal to

\[ \frac{q}{fd} \chi \left( \frac{mdf}{q} \right) \tau(\chi), \]

thus (11) and (6) give that

\[ \mathfrak{A} X_d = \frac{q}{fd} \tau(\chi) \bar{X}_{a/fd}. \] (12)

Using (12) we may write down a basis for the eigenvectors of \( \mathfrak{A}. \) If \( \chi \) is real and \( d^2 = q/f \), then (12) implies that \( X_d \) is an eigenvector of \( \mathfrak{A} \) corresponding to the eigenvalue \( (q/f)^{1/2} \tau(\chi) \). Otherwise let \( \lambda = \pm (\chi(-1)q)^{1/2} \), and consider the vector

\[ E(\chi, d, \lambda) = d^{1/2} X_d + \frac{\lambda}{\tau(\chi)} d^{1/2} \bar{X}_{a/fd}. \] (13)

By the lemma \( E(\chi, d, \lambda) \neq 0 \), and by (12) and (3) we have

\[ \mathfrak{A} E(\chi, d, \lambda) = \frac{q}{f} d^{1/2} \tau(\chi) \bar{X}_{a/fd} + \frac{\lambda}{\tau(\bar{\chi})} d^{1/2} d \tau(\bar{\chi}) X_d \]

\[ = \lambda \left( d^{1/2} X_d + \frac{q\tau(\chi)}{\lambda f} d^{1/2} \bar{X}_{a/fd} \right) \]

\[ = \lambda E(\chi, d, \lambda). \]

Thus \( E(\chi, d, \lambda) \) is an eigenvector of \( \mathfrak{A} \) corresponding to the eigenvalue \( \lambda \).

An easy computation using (13) shows that

\[ E(\bar{\chi}, q/fd, \lambda) = W(\chi, \lambda) E(\chi, d, \lambda), \] (14)
where $W(\chi, \lambda) = [\lambda/\tau(\chi)](f/q)^{1/2}$. Since $|\tau(\chi)| = f^{1/2}$, $W(\chi, \lambda)$ has absolute value 1, and $E(\chi, d, \lambda)$ and $E(\bar{\chi}, q/\lambda, \lambda)$ are dependent vectors. However the lemma implies easily that (14) is the only set of dependence relations between the vectors given in (13). It follows that a quadruple $(x, \bar{x}, d, q/\lambda)$ contributes the independent eigenvectors

$$E(\chi, d, \pm(\chi(-1)q)^{1/2}), E(\bar{\chi}, d, \pm(\chi(-1)q)^{1/2}), \quad \text{if } \chi \neq \bar{\chi}, d^2 \neq q/\ell;$$

$$E(\chi, d, \pm(\chi(-1)q)^{1/2}), \quad \text{if } \chi \neq \bar{\chi}, d^2 = q/\ell \text{ or } \chi = \bar{\chi}, d^2 \neq q/\ell; \quad (15)$$

$$X_d, \quad \text{if } \chi = \bar{\chi} \text{ and } d^2 = q/\ell.$$ 

By pairing the eigenvectors in (15) with the pairs $(\chi, d)$ $(d \mid q/\ell(\chi))$, it is easy to see that the total number of eigenvectors listed in (15) is

$$\sum_{\chi} \sum_{d \mid q/\ell(\chi)} 1 = \sum_{f \mid q} p(f) d(q/\ell) = q.$$ 

Hence we have the following result.

**Theorem.** The vectors listed in (15) (with $X_d$ and $E(\chi, d, \lambda)$ defined by (6) and (13)) form a basis of eigenvectors for $\mathfrak{A}$. The respective eigenvalues are

$$\pm(\chi(-1)q)^{1/2}, \pm(\chi(-1)q)^{1/2}, \text{and } \left(\frac{q}{\ell}\right)^{1/2} \tau(\chi),$$

where $\tau(\chi)$ is given by (2).

We note the following corollary of the theorem, which is a consequence of the fact that the trace of $\mathfrak{A}$ is equal to the sum of its eigenvalues:

$$S = \sum_{n=1}^{q} e^{2\pi in^3/q} = q^{1/2} \sum_{\chi \mid q/\ell(\chi)} \frac{\tau(\chi)}{\ell^{1/2}(\chi)}.$$ 

This can also be proved directly.

Similar results can also be proved for the matrix

$$\mathfrak{A}' = (e^{2\pi i S(\chi y n)}) \quad (x, y \pmod{q}),$$

where $S$ denotes the trace from a fixed algebraic number field $K$ to $\mathbb{Q}$, $q$ is some integral divisor of $K$, $x$ and $y$ are integers of $K$ which run through a complete residue system $(\mod{q})$, and $\eta$ satisfies

$$\eta = \frac{n}{q^d}, \quad (n, qd) = 1,$$
where \( b \) is the different of \( K/Q \) and \( n \) is an integral divisor in \( K \). As before, the eigenvectors of \( \Phi' \) arise from the characters on the reduced residue class group \((\text{mod } q)\) in \( K \).

**Acknowledgment**

Finally, I would like to thank Professor H. Montgomery for suggesting this problem to me.

**References**