Inversion of two cyclotomic matrices

Kurt Girstmair

Abstract
Let \( n \geq 3 \) be a square-free natural number. We explicitly describe the inverses of the matrices
\[
(2 \sin(2\pi jk^*/n))_{j,k} \quad \text{and} \quad (2 \cos(2\pi jk^*/n))_{j,k},
\]
where \( k^* \) denotes a multiplicative inverse of \( k \mod n \) and \( j, k \) run through the set \( \{l; 1 \leq l \leq n/2, (l, n) = 1\} \). These results are based on the theory of Gauss sums.

1. Introduction and results

In the paper [3] Lehmer states that there are only few classes of matrices for which explicit formulas for the determinant, the eigenvalues and the inverse are known. He gives a number of examples of this kind. Further examples can be found in the papers [1], [5] and [4]. The closest analogue of the matrices considered here is contained in the article [4], namely, the matrix
\[
(\sin(2\pi jk/n))_{j,k},
\]
where \( 1 \leq j, k \leq n, (jk, n) = 1 \). The author of [4] determines the characteristic polynomial of this matrix, the multiplicities of the eigenvectors being quite involved. In the present note we describe the eigenvalues of similar matrices \( S \) and \( C \). The main results, however, are explicit formulas for the inverses \( S^{-1} \) and \( C^{-1} \) in the cases when these matrices are invertible. This is in contrast to the papers we have quoted, since explicit formulas for inverses are scarcely given there.

Let \( n \geq 3 \) be a natural number. Let \( \mathcal{R} \) denote a system of representatives of the group \((\mathbb{Z}/zn)^\times/\{\pm 1\}\). Suppose that \( \mathcal{R} \) is ordered in some way. Typically, \( \mathcal{R} \) is the set \( \{k; 1 \leq k \leq n/2, (k, n) = 1\} \) with its natural order. For \( k \in \mathbb{Z}, (k, n) = 1 \), let \( k^* \) denote an inverse of \( k \mod n \) (so \( kk^* \equiv 1 \mod n \)). We define
\[
s_k = 2 \sin(2\pi k/n) \quad \text{and} \quad c_k = 2 \cos(2\pi k/n),
\]
where \( k \in \mathbb{Z}, (k, n) = 1 \). We consider the matrices
\[
S = (s_{jk^*})_{j,k \in \mathcal{R}} \quad \text{and} \quad C = (c_{jk^*})_{j,k \in \mathcal{R}},
\]
which we call the \textit{sine matrix} and the \textit{cosine matrix}, respectively.

We think that the matrices \( S \) and \( C \) deserve some interest not only because of their simple structure but also by reason of their connection with cyclotomy, in particular, with Gauss sums (see [6] for the history of this topic).

In order to be able to enunciate our main results, we define
\[
\lambda(k) = |\{q; q \geq 3, q \mod n, k \equiv 1 \mod q\}| \quad (1)
\]
for $k \in \mathbb{Z}$, $(k, n) = 1$. Furthermore, put
\[
\hat{s}_k = \frac{1}{n} \sum_{l \in \mathbb{R}} (\lambda(lk) - \lambda(-lk))s_l, \tag{2}
\]
for $k \in \mathbb{Z}$, $(k, n) = 1$. For the same numbers $k$ put
\[
\hat{c}_k = \frac{1}{n} \sum_{l \in \mathbb{R}} (\lambda(lk) + \lambda(-lk) + \rho_n)c_l, \tag{3}
\]
with
\[
\rho_n = \begin{cases} 
2, & \text{if } n \text{ is odd;} \\
4, & \text{if } n \text{ is even.} 
\end{cases} \tag{4}
\]
Our main results are as follows.

**Theorem 1** The sine matrix $S$ is invertible if, and only if, $n$ is square-free or $n = 4$. In this case
\[
S^{-1} = (\hat{s}_{jk^*})_{j,k \in \mathbb{R}},
\]
with $\hat{s}_{jk^*}$ defined by (2).

**Theorem 2** The cosine matrix $C$ is invertible if, and only if, $n$ is square-free. In this case
\[
C^{-1} = (\hat{c}_{jk^*})_{j,k \in \mathbb{R}}
\]
with $\hat{c}_{jk^*}$ defined by (3).

The entries of $S$ have the form $\pm s_l$, $l \in \mathbb{R}$. This is due to the fact that
\[
s_{jk^*} = \varepsilon s_l
\]
with $\varepsilon \in \{\pm 1\}$, $l \in \mathbb{R}$, if $jk^* \equiv \varepsilon l \mod n$. In the same way we have
\[
\hat{s}_{jk^*} = \varepsilon \hat{s}_l
\]
if $jk^* \equiv \varepsilon l \mod n$. This means that it suffices to compute the numbers $\hat{s}_l$ only for $l \in \mathbb{R}$ in order to write down the matrix $S^{-1}$. Indeed, this matrix arises from $S$ if we replace each entry $\varepsilon s_l$ of $S$ by the respective entry $\varepsilon \hat{s}_l$.

The same procedure works in the case of the cosine matrix, whose entries have the form $c_l$, $l \in \mathbb{R}$.

**Example.** Let $n = 15$ and $\mathbb{R} = \{1, 2, 4, 7\}$. Then $S$ can be written
\[
S = \begin{pmatrix}
    s_1 & -s_7 & s_4 & -s_2 \\
    s_2 & s_1 & -s_7 & -s_4 \\
    s_4 & s_2 & s_1 & s_7 \\
    s_7 & -s_4 & -s_2 & s_1
\end{pmatrix} \tag{5}
\]
Theorem\[ yields $\hat{s}_1 = (3s_1 - s_2 + s_7)/15$, $\hat{s}_2 = (-s_1 - s_4 - 3s_7)/15$, $\hat{s}_4 = (-s_2 + 3s_4 + s_7)/15$, and $\hat{s}_7 = (s_1 - 3s_2 + s_4)/15$. We obtain $S^{-1}$ if we put a circumflex on each $s$ occurring in (5).
Remark. If $n = p$ is a prime, Theorem 1 shows that $S^{-1}$ is particularly simple, namely, $S^{-1} = \frac{1}{p} S^t$ ($S^t$ is the transpose of $S$). There is no analogue for the cosine matrix. For instance, if $p = 7$ and $\mathcal{R} = \{1, 2, 3\}$, we have $\hat{c}_1 = (3c_1 + 2c_2 + 2c_3)/7$. The prime number case of the sine matrix can also be settled by means of a simple trigonometric argument. This, however, seems to be hardly possible if $n$ consists of at least two prime factors $p > q \geq 3$.

2. Proofs

First we prove Theorem 1, then we indicate the changes required by the proof of Theorem 2. Let $\mathcal{X}$ denote the set of Dirichlet characters mod $n$, and $\mathcal{X}^-$ and $\mathcal{X}^+$ the subsets of odd and even characters, respectively. The matrix $S$ is connected with $\mathcal{X}^-$, whereas $C$ is connected with $\mathcal{X}^+$. We note the orthogonality relation

$$\sum_{\chi \in \mathcal{X}^-} \chi(k) = \begin{cases} 0, & \text{if } k \not\equiv \pm1 \mod n; \\ \varphi(n)/2, & \text{if } k \equiv 1 \mod n; \\ -\varphi(n)/2, & \text{if } k \equiv -1 \mod n, \end{cases}$$

(6)

see [2, p. 210]. Here $(k, n) = 1$ and $\varphi$ denotes Euler’s function.

Suppose that the set $\mathcal{X}^-$ is ordered in some way. Then we can define the matrix

$$X = \sqrt{n/\varphi(n)}(\chi(k))_{k \in \mathcal{R}, \chi \in \mathcal{X}^-}.$$

Since $|\mathcal{R}| = |\mathcal{X}^-| = \varphi(n)/2$, $X$ is a square matrix. We note the following lemma.

Lemma 1 The matrix $X$ is unitary, i.e., $X^{-1} = X^t$ (the transpose of the complex-conjugate matrix).

Proof. This is an immediate consequence of the orthogonality relation (6) (observe that $\chi^* = \chi^t$).

Let $\zeta_n = e^{2\pi i/n}$ be the standard primitive $n$th root of unity. For $\chi \in \mathcal{X}^-$ let

$$\tau(\chi) = \sum_{k=1}^{n} \chi(k)\zeta_n^k$$

(7)

the corresponding Gauss sum, see [2, p. 445]. We consider the diagonal matrix

$$T = \text{diag}(\tau(\chi))_{\chi \in \mathcal{X}^-}.$$

Proposition 1 The sine matrix $S$ is normal. Indeed,

$$\overline{X^t}SX = -iT.$$

Proof. We show $XT\overline{X} = iS$. Obviously, the entry $(XT\overline{X})_{j,k}$ equals

$$\frac{2}{\varphi(n)} \sum_{\chi \in \mathcal{X}^-} \chi(j)\tau(\chi)\overline{\chi(k)} = \frac{2}{\varphi(n)} \sum_{\chi \in \mathcal{X}^-} \chi(jk^*) \sum_{(l,n)=1} \chi(l^*) \zeta_n^l,$$
where the index $l$ satisfies $1 \leq l \leq n$, $(l, n) = 1$. This can be written

$$\frac{2}{\varphi(n)} \sum_{l=1}^{\varphi(n)} \zeta_n^l \sum_{\chi \in \mathcal{X}} \chi(jk^*l^*).$$

Now the orthogonality relation (6), together with $\zeta_n^l - \zeta_n^{-l} = is_l$, shows that this is just $is_{jk^*}$.

In order to study the vanishing of the eigenvalues of $S$, we use the reduction formula

$$\tau(\chi) = \mu \left( \frac{n}{f_\chi} \right) \tau_f \left( \frac{n}{f_\chi} \right) \tau(\chi_f),$$

(8) see [2, p. 448]. Here $\mu$ means the Möbius function, $f_\chi$ the conductor of the character $\chi$, $\chi_f$ the primitive character belonging to $\chi$ (which is a Dirichlet character mod $f_\chi$) and $\tau(\chi_f)$ the Gauss sum

$$\sum_{k=1}^{f_\chi} \chi_f(k) \zeta_{f_\chi}^k.$$

Since

$$\tau(\chi_f) \tau(\chi_f) = -f_\chi$$

(9) (see [2, p. 269]), formula (8) shows when the eigenvalue $-i\tau(\chi)$ vanishes. We obtain the following result.

**Proposition 2** The matrix $S$ is invertible if, and only if, $n$ is square-free or $n = 4$.

**Proof.** If $n$ is square-free, then $n/f_\chi$ is square-free and $(f_\chi, n/f_\chi) = 1$. By (8) and (9), all Gauss sums $\tau(\chi)$ are different from 0. If $n = 4$ and $\chi \in \mathcal{X}^-$, then $f_\chi = 4$ and $n/f_\chi = 1$.

Conversely, suppose that $n$ is not square-free and different from 4. Then one of the following three cases occurs. There is a prime $p \geq 3$ such that $p^2 \mid n$, or $4p \mid n$, or $8 \mid n$. In the first and the second case there is a character $\chi \in \mathcal{X}^-$ with $f_\chi = p$. Accordingly, $\chi_f(n/f_\chi) = 0$ or $\mu(n/f_\chi) = 0$. In the third case there is a character $\chi \in \mathcal{X}^-$ with $f_\chi = 4$. Therefore, $\chi_f(n/f_\chi) = 0$. □

**Lemma 2** Let $n$ be square-free or equal to 4. For $k \in \mathbb{Z}$, $(k, n) = 1$, we have

$$\sum_{\chi \in \mathcal{X}^-} \frac{\chi(k)}{f_\chi} = \frac{\varphi(n)}{2n} \left( \lambda(k) - \lambda(-k) \right),$$

the $\lambda$’s being defined by (1).

**Proof.** Obviously,

$$\sum_{\chi \in \mathcal{X}^-} \frac{\chi(k)}{f_\chi} = \sum_{d \mid n} \frac{1}{d} \sum_{\chi \in \mathcal{X}^-} \chi(k).$$

Möbius inversion gives

$$\sum_{\chi \in \mathcal{X}^-} \chi(k) = \sum_{d \mid n} \mu \left( \frac{d}{q} \right) \sum_{f_\chi = d} \chi(k).$$
Here we note that the characters \( \chi \in \mathcal{X}^- \) with \( f_x \mid q \) are in one-to-one correspondence with the odd Dirichlet characters mod \( q \). Indeed, if \( \chi \in \mathcal{X}^- \), one defines the Dirichlet character \( \chi_q \) mod \( q \) in the following way. If \((j,q) = 1\), there is an integer \( l \) with \((l,n) = 1\) such that \( l \equiv j \mod q \). Then \( \chi_q(j) = \chi(l) \), see [2, p. 217]. Accordingly,

\[
\sum_{f_x \mid q} \chi(k) = \sum_{\chi_q} \chi_q(k).
\]

From (6) we obtain

\[
\sum_{\chi_q} \chi(k) = \begin{cases} 
0, & \text{if } q \leq 2 \text{ or } q \geq 3 \text{ and } k \not\equiv \pm 1 \mod q; \\
\frac{\varphi(q)}{2}, & \text{if } q \geq 3 \text{ and } k \equiv 1 \mod q; \\
-\frac{\varphi(q)}{2}, & \text{if } q \geq 3 \text{ and } k \equiv -1 \mod q 
\end{cases}
\]  

(10)

(observe that there are no odd characters \( \chi_q \) if \( q \leq 2 \)). Therefore, we have

\[
\sum_{\chi \in \mathcal{X}^-} \frac{\chi(k)}{f_x} = \sum_{q \mid d,q \geq 3, k \equiv \pm 1 \mod q} \pm \mu \left( \frac{d}{q} \right) \frac{\varphi(q)}{2},
\]

where the \( \pm \) sign in the summand corresponds to the respective sign in the summation index. If we write \( d = q \cdot r \), we have

\[
\sum_{\chi \in \mathcal{X}^-} \frac{\chi(k)}{f_x} = \sum_{q \mid n,q \geq 3, k \equiv \pm 1 \mod q} \pm \frac{\varphi(q)}{2} \sum_{r \mid n,q} \frac{\mu(r)}{qr}.
\]

Since

\[
\sum_{r \mid n,q} \frac{\mu(r)}{r} = \prod_{p \mid n,q} \left( 1 - \frac{1}{p} \right) = \frac{\varphi(n)/q}{n/q}
\]

we obtain

\[
\sum_{\chi \in \mathcal{X}^-} \frac{\chi(k)}{f_x} = \sum_{q \mid n,q \geq 3, k \equiv \pm 1 \mod q} \pm \frac{\varphi(q)}{2q} \cdot \frac{\varphi(n)/q}{n/q}.
\]  

(11)

However, \( n \) is square-free or equal to 4, and so \( \varphi(q)\varphi(n/q) = \varphi(n) \). This implies

\[
\sum_{\chi \in \mathcal{X}^-} \frac{\chi(k)}{f_x} = \frac{\varphi(n)}{2n} (\lambda(k) - \lambda(-k)).
\]

\[ \Box \]

**Proof of Theorem** 4  By Proposition 4 \( S^{-1} = iXT^{-1}X^* \), which means that the entry \((S^{-1})_{j,k} \), \( j,k \in \mathcal{R} \), of \( S^{-1} \) is given by

\[
(S^{-1})_{j,k} = \frac{2i}{\varphi(n)} \sum_{\chi \in \mathcal{X}^-} \chi(j)\tau(\chi)^{-1} \tau(\chi(k)).
\]

From (8) and (9) we obtain

\[
\tau(\chi)^{-1} = \frac{\mu(n/f_x)\chi_f(n/f_x)\tau(\chi_f)}{-f_x} = -\frac{\tau(\chi)}{f_x}.
\]
Therefore,

\[(S^{-1})_{j,k} = \frac{-2i}{\varphi(n)} \sum_{\chi \in \mathcal{X}^-} \frac{\chi(jk^*)}{f_\chi} \tau(\chi).\]

Now (7) yields

\[(S^{-1})_{j,k} = \frac{-2i}{\varphi(n)} \sum_{(l,n)=1} \zeta_n^l \zeta_n^{-l} \sum_{\chi \in \mathcal{X}^-} \frac{\chi(ljk^*)}{f_\chi}.\]

By Lemma 2

\[(S^{-1})_{j,k} = \frac{-2i}{\varphi(n)} \sum_{(l,n)=1} \zeta_n^l \varphi(n) \frac{\varphi(n)}{2n} (\lambda(ljk^*) - \lambda(-ljk^*)).\]

Altogether, we have

\[(S^{-1})_{j,k} = \frac{-i}{n} \sum_{(l,n)=1} \zeta_n^l (\lambda(ljk^*) - \lambda(-ljk^*)).\]

On observing that \(s_l = -i(\zeta_n^l - \zeta_n^{-l})\), we obtain Theorem 1.

\[\square\]

The setting of the proof of Theorem 2 is slightly different. Indeed, the unitary matrix \(X\) is defined by

\[X = \sqrt{n/\varphi(n)}(\chi(k))_{k \in \mathbb{R}, \chi \in \mathcal{X}^+}.\]

The cosine matrix \(C\) is normal, and \(X^t CX = T\), with \(T = \text{diag}(\tau(\chi))_{\chi \in \mathcal{X}^+}\). In this case it is easy to see that \(T\) (and, hence, \(C\)) is invertible if, and only if, \(n\) is square-free. Instead of (9) we have

\[\tau(\chi_f)\tau(\chi_f) = f_\chi.\]

The analogue of Lemma 2 reads

\[\sum_{\chi \in \mathcal{X}^+} \frac{\chi(k)}{f_\chi} = \frac{\varphi(n)}{2n} (\lambda(k) + \lambda(-k) + \rho_n) \quad (12)\]

with \(\rho_n\) as in (11). This is due to the fact that the counterpart of formula (10) takes the form

\[\sum_{\chi} \chi(q) = \begin{cases} 
1, & \text{if } q \leq 2; \\
0, & \text{if } q \geq 3 \text{ and } k \not\equiv \pm1 \text{ mod } q; \\
\varphi(q)/2, & \text{if } q \geq 3 \text{ and } k \equiv \pm1 \text{ mod } q.
\end{cases}\]

Accordingly, formula (11) has the equivalent

\[\sum_{\chi \in \mathcal{X}^+} \frac{\chi(k)}{f_\chi} = \sum_{\varphi(q) \mid n, q \geq 3} \frac{\varphi(q)}{2q} \cdot \frac{\varphi(n/q)}{n/q} + \sum_{d\mid n, 2\mid d} \frac{\mu(d)}{d},\]

which gives (12). Up to these differences, the proof follows the pattern of the proof of Theorem 1.
References

[1] L. Carlitz, Some cyclotomic matrices, Acta Arith. 5 (1959), 293–308.

[2] H. Hasse, Vorlesungen über Zahlentheorie (2nd ed.), Springer, Berlin 1964.

[3] D. H. Lehmer, On certain character matrices, Pacif. J. Math. 6 (1956), 491–499.

[4] G. Molteni, About two trigonometric matrices, Lin. Alg. Appl. 382 (2004), 39–59.

[5] P. Morton, On the eigenvectors of Schur’s matrix, J. Number Th. 12 (1980), 122–127.

[6] A. Weil, La cyclotomie jadis et naguère, Sém. Bourbaki 1973-74, exp. nr. 452, 318–338.

Kurt Girstmair
Institut für Mathematik
Universität Innsbruck
Technikerstr. 13/7
A-6020 Innsbruck, Austria
Kurt.Girstmair@uibk.ac.at