Electronic Research Archive

https://www.aimspress.com/journal/era

ERA, 32(7): 4741–4752.
DOI: 10.3934/era.2024216
Received: 18 June 2024
Revised: 16 July 2024
Accepted: 19 July 2024
Published: 30 July 2024

Research article

Determinants and invertibility of circulant matrices

Xiuyun Guo[1,2,*] **and Xue Zhang**[1]

[1] College of Mathematics and Systems Science, Shandong University of Science and Technology, Qingdao 266590, China

[2] Department of Mathematics, Shanghai University, Shanghai 200444, China

* **Correspondence:** Email: xyguo@shu.edu.cn.

Abstract: Let $a_0, a_1, \ldots, a_{n-1}$ be real numbers and let $A = Circ(a_0, a_1, \ldots, a_{n-1})$ be a circulant matrix with $f(x) = \Sigma_{j=0}^{n-1} a_j x^j$. First, we prove that $Circ(a_0, a_1, \ldots, a_{n-1})$ must be invertible if the sequence $a_0, a_1, \ldots, a_{n-1}$ is a strictly monotonic sequence and $a_0 + a_1 + \cdots + a_{n-1} \neq 0$. Next, we reduce the calculation of $f(\varepsilon^0) f(\varepsilon) \ldots f(\varepsilon^{n-1})$ for a prime n by using the techniques on finite fields, where ε is a primitive n-th root of unity. Finally, we provide two examples to explain how to use the obtained results to calculate the determinant of a circulant matrix.

Keywords: circulant matrix; invertibility of circulant matrix; determinant; primitive n-th root of unity; strictly monotonic sequence

1. Introduction

Circulant matrices are a kind of important patterned matrix which arises in many areas of physics, molecular vibration, signal processing, image processing, digital image disposal, error correcting code theory, and applied mathematics [1–3]. Consequently, there are many papers that investigated the properties and applications of circulant matrices. In order to better understand the essence of circulant matrices, in recent years, some scholars have tried to provide an effective expression for the determinant, the eigenvalues, and the corresponding inverses, see for instance [4–7]. On the other hand, the invertibility of circulant matrices has been widely studied in the literature by using the primitive n-th root of unity and some associated polynomial, see [7, 8]. In fact, circulant matrices $Circ(a_0, a_1, \cdots, a_{n-1})$ are invertible if and only if $f(\varepsilon^j) \neq 0$ for every $0 \leq j \leq n-1$, where $f(x) = \Sigma_{j=0}^{n-1} a_j x^j$ and ε is a primitive n-th root of unity. However, it is not easy to count the product $f(\varepsilon^0) f(\varepsilon) \cdots f(\varepsilon^{n-1})$, see [4]. Therefore, it is important to either reduce the calculation of $f(\varepsilon^0) f(\varepsilon) \cdots f(\varepsilon^{n-1})$ or to provide other criteria for discrimination. Recently, the authors in [4] investigated circulant matrices of type $Circ(a, b, c, \cdots, c)$ and $Circ(a, b, c, \cdots, c, b)$ and provided some necessary and sufficient conditions for its invertibility. Furthermore, they explicitly obtained a closed formula for the inverse matrices of these type of circulant matrices.

In this paper, we first consider circulant matrices of type $Circ(a_0, a_1, \cdots, a_{n-1})$ with $a_0, a_1, \cdots, a_{n-1}$ a strictly monotonic sequence. This type of matrix arises in the study of sum systems and sum circulant matrices. A sum system is a collection of finite sets of integers such that the sums formed by taking one element from each set generates a prescribed arithmetic progression, and a sum circulant matrix whose left and right circulant parts take their entries from the two component sets of a sum system has consecutive integer entries, for example, see [9–11]. We prove that this kind of circulant matrix must be invertible. Next, we hope to reduce the calculation of $f(\varepsilon^0)f(\varepsilon)\cdots f(\varepsilon^{n-1})$ for a prime n by using the techniques on finite fields to calculate the determinant of a circulant matrix by a simple program. Finally, we provide two examples to explain how to use the obtained results to calculate the determinant of a circulant matrix.

2. Prelemanery

In this section, we recall some basic concepts and provide some results needed during the proof of our main theorems.

A matrix $A = (a_{ij})$ is said to be circulant (or right circulant) with parameters $a_0, \cdots, a_{n-1}$ if

$$A = \begin{pmatrix} a_0 & a_1 & \dots & a_{n-2} & a_{n-1} \\ a_{n-1} & a_0 & \dots & a_{n-3} & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_2 & a_3 & \dots & a_0 & a_1 \\ a_1 & a_2 & \dots & a_{n-1} & a_0 \end{pmatrix}.$$

It is usually abbreviated as $A = Circ(a_0, a_1, \ldots, a_{n-1})$. It is clear that $Circ(a_0, a_1, \ldots, a_{n-1}) = a_0P^0 + a_1P^1 + a_2P^2 + \ldots + a_{n-1}P^{n-1}$ with $P = Circ(0, 1, 0, \ldots, 0)$ and $P^0 = I$.

Let ε be a primitive n-th root of unity. Then, $1 = \varepsilon^0, \varepsilon, ..., \varepsilon^{n-1}$ are different from each other, that is, they are just all n-th roots of unity.

The following results are well-known, and can be found in [2].

Lemma 2.1. *Let $A = Circ(a_0, a_1, \ldots, a_{n-1})$ be a circulant matrix, ε be a primitive n-th root of unity, and $f(x) = \Sigma_{j=0}^{n-1} a_j x^j$. Then,*

1) $|A| = \Pi_{j=0}^{n-1} f(\varepsilon^j)$;

2) A is invertible if and only if $f(\varepsilon^j) \neq 0$ for $j = 0, 1, \cdots, n-1$; and

3) If A is invertible, then the inverse A^{-1} of A is also a circulant matrix.

Lemma 2.2. *Let n be a prime and ε be a n-th root of unity with $n \neq 1$. Then,*

1) ε must be a primitive n-th root of unity, and therefore $1 = \varepsilon^0, \varepsilon, ..., \varepsilon^{n-1}$ are all n-th roots of unity.

2) $Z_n = Z/\langle n \rangle$ is a field.

3. Circulant matrices $Circ(a_0, a_1, \ldots, a_{n-1})$ with $a_0, a_1, \ldots, a_{n-1}$ a strictly monotonic sequence

In this section, we prove that circulant matrices $Circ(a_0, \ldots, a_{n-1})$ must be invertible if $a_0, \ldots, a_{n-1}$ is a strictly monotonic sequence and $a_0 + a_1 + \cdots + a_{n-1} \neq 0$. If $a_0, a_1, \ldots, a_{n-1}$ are complex, then we also provide a condition for $Circ(a_0, \ldots, a_{n-1})$ to be invertible.

Lemma 3.1. *Let z and w be two non-zero complex numbers. Then, $|z + w| = |z| + |w|$ if and only if $z/w>0$.*

Proof. In fact, since $(|z| + |w|)^2 = |z|^2 + 2|z||w| + |w|^2$ and $|z + w|^2 = (z + w)(\bar{z} + \bar{w}) = |z|^2 + \bar{z}w + z\bar{w} + |w|^2$, we see $|z + w| = |z| + |w|$ if and only if $Re(\bar{w}z) = |z||w| = |\bar{w}z|$. Additionally, $Re(\bar{w}z) = |z||w| = |\bar{w}z|$ if and only if $z/w>0$. The proof is complete. □

Lemma 3.2. *Let z_1 and z_2 be two non-zero complex numbers. Then, $|z_1 + z_2| = |z_1| + |z_2|$ if and only if there is a complex number z and the real numbers $t_1 > 0$ and $t_2 > 0$ such that $z_1 = t_1 z$, $z_2 = t_2 z$.*

Proof. It is an immediate consequence of Lemma 3.1. □

Lemma 3.3. *Let $z_1, z_2, \ldots, z_s$ be non-zero complex numbers. Then, $|z_1+z_2+\cdots+z_s| = |z_1|+|z_2|+\cdots+|z_s|$ if and only if there is a complex number z and the real numbers $t_j > 0$ such that $z_j = t_j z$ $(j = 1, 2, \ldots, s)$.*

Proof. The sufficiency clearly holds; therefore, we only need to prove the necessity. Since $|z_1| + \cdots + |z_s| = |z_1 + \cdots + z_s| \le |z_1| + |z_2 + \cdots + z_s| \le |z_1| + \cdots + |z_s|$, we see the following:

$$|z_1 + \cdots + z_s| = |z_1| + |z_2 + \cdots + z_s|.$$

and

$$|z_2 + \cdots + z_s| = |z_2| + \cdots + |z_s|.$$

By Lemma 3.2, there are $m_1 > 0, m_2 > 0$, and a complex number u such that $z_1 = m_1 u, z_2+\cdots+z_s = m_2 u$. By induction, there is a complex number z and real numbers $t_j > 0$ such that $z_j = t_j z$ $(j = 2, \ldots, s)$.

Obviously $u \neq 0 \neq z$, and

$$\begin{aligned} |z + u| &= |1/(t_2 + \cdots + t_s)(z_2 + \cdots + z_s) + 1/m_2(z_2 + \cdots + z_s)| \\ &= 1/(t_2 + \cdots + t_s)|z_2 + \cdots + z_s| + 1/m_2|z_2 + \cdots + z_s| \\ &= |z| + |u|. \end{aligned}$$

By Lemma 3.1, we see $u/z > 0$, therefore, $t_1 = m_1(u/z) > 0$ and $z_1 = t_1 z$. □

Lemma 3.4. *Let $f(x) = z_0 + z_1 x + \cdots + z_{n-1}x^{n-1}$ be a complex coefficient polynomial with $n > 2$, ε be a root of $x^n = 1$, and $\varepsilon \neq 1$. If there exist real numbers $t_j > 0$ and a non-zero complex number z such that $z_j - z_{j+1} = t_j z$ $(j = 0, 1, \ldots, n-2)$, then $f(\varepsilon) \neq 0$.*

Proof. Let $S_0 = 1, S_k = 1 + \varepsilon + \cdots + \varepsilon^k$ for $k = 1, 2, \ldots, n-1$. Then, the following holds:

$$\begin{aligned} f(\varepsilon) &= z_0 + z_1\varepsilon + \cdots + z_{n-1}\varepsilon^{n-1} \\ &= z_0 S_0 + z_1(S_1 - S_0) + z_2(S_2 - S_1) + \cdots + z_{n-1}(S_{n-1} - S_{n-2}) \\ &= (z_0 - z_1)S_0 + (z_1 - z_2)S_1 + \cdots + (z_{n-2} - z_{n-1})S_{n-2} + z_{n-1}S_{n-1}. \end{aligned}$$

Noticing that $(1+\varepsilon+\cdots+\varepsilon^{n-1})(1-\varepsilon) = 1-\varepsilon^n = 0$ and $\varepsilon \neq 1$, we see $S_{n-1} = 1+\varepsilon+\cdots+\varepsilon^{n-1} = 0$. Therefore,

$$\begin{aligned} f(\varepsilon) &= (z_0 - z_1)S_0 + (z_1 - z_2)S_1 + \cdots + (z_{n-2} - z_{n-1})S_{n-2} \\ &= (z_0 - z_1) + (z_1 - z_2)(1-\varepsilon^2)/(1-\varepsilon) + \cdots + \\ &+ (z_{n-2} - z_{n-1})(1-\varepsilon^{n-1})/(1-\varepsilon) \\ &= 1/(1-\varepsilon)[(z_0 - z_1)(1-\varepsilon) + (z_1 - z_2)(1-\varepsilon^2) + \cdots + \\ &+ (z_{n-2} - z_{n-1})(1-\varepsilon^{n-1})] \\ &= 1/(1-\varepsilon)[(z_0 - z_1) + \cdots + (z_{n-2} - z_{n-1}) - \\ &- (z_0 - z_1)\varepsilon - (z_1 - z_2)\varepsilon^2 - \cdots - (z_{n-2} - z_{n-1})\varepsilon^{n-1}] \\ &= 1/(1-\varepsilon)[z_0 - z_{n-1} - (z_0 - z_1)\varepsilon - \cdots - (z_{n-2} - z_{n-1})\varepsilon^{n-1}]. \end{aligned}$$

Since ε is a root of $x^n = 1$ and $\varepsilon \neq 1$, ε is either -1 or a complex number; therefore, $(z_1 - z_2)\varepsilon/(z_0 - z_1) = t_1\varepsilon/t_0$ is either negative or a complex number. By using Lemma 3.3, we have the following:

$$\begin{aligned} &|(z_0 - z_1)\varepsilon + (z_1 - z_2)\varepsilon^2 + \cdots + (z_{n-2} - z_{n-1})\varepsilon^{n-1}| \\ &< |(z_0 - z_1)\varepsilon| + |(z_1 - z_2)\varepsilon^2| + \cdots + |(z_{n-2} - z_{n-1})\varepsilon^{n-1}| \\ &= |(z_0 - z_1)||\varepsilon| + |(z_1 - z_2)||\varepsilon^2| + \cdots + |(z_{n-2} - z_{n-1})||\varepsilon^{n-1}| \\ &= |(z_0 - z_1)| + |(z_1 - z_2)| + \cdots + |(z_{n-2} - z_{n-1})|. \end{aligned}$$

Now, by the hypothesis and Lemma 3.3, we observe the following:
$|(z_0 - z_1)| + |(z_1 - z_2)| + \cdots + |(z_{n-2} - z_{n-1})| = |(z_0 - z_1) + (z_1 - z_2) + \cdots + (z_{n-2} - z_{n-1})| = |z_0 - z_{n-1}|$, so

$$\begin{aligned} |f(\varepsilon)| &= |1/(1-\varepsilon)||z_0 - z_{n-1} - (z_0 - z_1)\varepsilon - \cdots - (z_{n-2} - z_{n-1})\varepsilon^{n-1}| \\ &\geq |1/(1-\varepsilon)|[|z_0 - z_{n-1}| - |(z_0 - z_1)\varepsilon + \cdots + (z_{n-2} - z_{n-1})\varepsilon^{n-1}|] \\ &> |1/(1-\varepsilon)|[|z_0 - z_{n-1}| - |z_0 - z_{n-1}|] = 0. \end{aligned}$$

Hence, $f(\varepsilon) \neq 0$.

□

Corollary 3.1. *Let $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ be a real coefficient polynomial with $n > 2$, ε be a root of $x^n = 1$, and $\varepsilon \neq 1$. If the sequence $a_0, a_1, \ldots, a_{n-1}$ is either strictly increasing or strictly decreasing, then $f(\varepsilon) \neq 0$.*

Proof. It is immediate consequence of Lemma 3.4. □

By Lemma 3.4 and Corollary 3.1, we may state our main results in this section.

Theorem 3.1. *Let $A = Circ(a_0, a_1, \ldots, a_{n-1})$ be a circulant matrix with $a_0 + a_1 + \cdots + a_{n-1} \neq 0$.*

1) If $a_0, a_1, \ldots, a_{n-1}$ are real numbers and the sequence $a_0, a_1, \ldots, a_{n-1}$ is either strictly increasing or strictly decreasing, then A is invertible.

2) If $a_0, a_1, \ldots, a_{n-1}$ are complex numbers and there exist real numbers $t_j > 0$ and a non-zero complex numbers z such that $a_j - a_{j+1} = t_jz$ $(j = 0, 1, \ldots, n-2)$, then A is invertible.

4. Circulant matrices with a prime order

In this section, we always assume that $a_0, a_1, \cdots, a_{n-1}$ is a sequence of real numbers and that $A = Circ(a_0, a_1, \cdots, a_{n-1})$ is a circulant matrix with a prime n. We try to reduce the calculation of $f(\varepsilon^0)f(\varepsilon)\cdots f(\varepsilon^{n-1})$, where ε is an n-th root of unity with $\varepsilon \neq 1$ and $f(x) = \Sigma_{j=0}^{n-1} a_j x^j$. It is clear that $f(\varepsilon^0)f(\varepsilon)\cdots f(\varepsilon^{n-1})$ is easy to calculate for either $n = 2$ or $n = 3$. Now, we assume that $n \geq 5$. For clarity, we first recall

$$\Delta = f(1)f(\varepsilon)\cdots f(\varepsilon^{n-1})$$

with

$$\begin{aligned}
f(1) &= a_0 + a_1 + a_2 + \cdots + a_{n-1} \\
f(\varepsilon) &= a_0 + a_1\varepsilon + a_2\varepsilon^2 + \cdots + a_{n-1}\varepsilon^{n-1} \\
&\vdots \\
f(\varepsilon^j) &= a_0 + a_1\varepsilon^j + a_2\varepsilon^{j\cdot 2} + \cdots + a_{n-1}\varepsilon^{j\cdot(n-1)} \\
&\vdots \\
f(\varepsilon^{n-1}) &= a_0 + a_1\varepsilon^{n-1} + a_2\varepsilon^{(n-1)\cdot 2} + \cdots + a_{n-1}\varepsilon^{(n-1)\cdot(n-1)}
\end{aligned}$$

Noticing that $\{(\varepsilon^j)^k | 0 \leq k \leq n-1\} = \{1, \varepsilon, \cdots, \varepsilon^{n-1}\}$ for every $1 \leq j \leq n-1$, we see that every $f(\varepsilon^j)$ can be seen as an $n-1$-degree polynomial in variable ε. Then, Δ is an algebraic sum containing n^n items, in which each term is the product of n monomials and every monomial comes from one and only one in $f(\varepsilon^j)$ for $j = 0, 1, \cdots, n-1$. Thus, the coefficient of each term in Δ can be written as follows:

$$a_{k_0}a_{k_1}a_{k_2}\ldots a_{k_j}\ldots a_{k_{n-1}},$$

where a_{k_j} is the coefficient of $(\varepsilon^j)^{k_j}$ in $f(\varepsilon^j)$. We should notice that a_{k_j} can take values of $a_0, a_1, \ldots, a_{n-1}$ for every $0 \leq j \leq n-1$ and the subscript k_j in a_{k_j} only indicates that a_{k_j} is taken from a certain coefficient of $f(\varepsilon^j)$. In this case, the corresponding degree of ε for this term in Δ is $0 \times k_0 + 1 \times k_1 + \cdots + i \times k_i + \cdots + (n-1) \times k_{n-1} (modn)$. In other words, every term and the corresponding coefficient of the term in Δ satisfies the following:

$$\begin{gathered}
a_{k_0}a_{k_1}a_{k_2}\ldots a_{k_j}\ldots a_{k_{n-1}} can\ become\ a\ coefficient\ of\ \varepsilon^i\ for\ i = 0, 1, \cdots, n-1 \\
\Longleftrightarrow \\
0 \times k_0 + 1 \times k_1 + 2 \times k_2 + \cdots + i \times k_i + \cdots + (n-1) \times k_{n-1} \equiv i (modn)
\end{gathered} \tag{4.1}$$

For simplicity, we use $[i; k_0, k_1, \ldots, k_{n-1}]$ to represent $0 \times k_0 + 1 \times k_1 + 2 \times k_2 + \cdots + i \times k_i + \cdots + (n-1) \times k_{n-1} \equiv i(modn)$.

Now, we merge items in Δ according to the degree of ε. Then, we have the following:

$$\Delta = b_0 + b_1\varepsilon + \cdots + b_i\varepsilon^i + \cdots + b_{n-1}\varepsilon^{n-1} \tag{4.2}$$

and

$$\sum_{[i;k_0,k_1,\ldots,k_{n-1}]} a_{k_0}a_{k_1}a_{k_2}\ldots a_{k_i}\ldots a_{k_{n-1}} = b_i \tag{4.3}$$

Therefore, determining the value of b_i is equivalent to studying all possibility of $k_0, k_1, \ldots, k_{n-1}$ satisfying Eq (4.1). Now, we first claim the following:

Claim 1. $b_i = b_j$ when $i \neq 0$ and $j \neq 0$.

In fact, if $a_{k_0} a_{k_1} a_{k_2} \ldots a_{k_{n-1}}$ with $0 \leq k_s \leq n-1$ is one term in b_i, then

$$0 \times k_0 + 1 \times k_1 + 2 \times k_2 + \cdots + i \times k_i + \cdots + (n-1) \times k_{n-1} \equiv i (modn)$$

Since $(i, n) = 1$ and $(j, n) = 1$, there exists $1 \leq t \leq n-1$ such that $it \equiv j(modn)$, then, $0 \times k_0 \times t + 1 \times k_1 \times t + \cdots + i \times k_i \times t + \cdots + (n-1) \times k_{n-1} \times t \equiv it \equiv j(modn)$,
that is

$$k_0 \times (0 \times t) + k_1 \times (1 \times t) + \cdots + k_{n-1} \times ((n-1) \times t) \equiv j(modn) \tag{4.4}$$

It follows from $1 \leq t \leq n-1$ that $(t, n) = 1$; therefore

$$\{0 \times t, 1 \times t, 2 \times t, \ldots, (n-1) \times t\} = \{0, 1, 2, \ldots, n-1\} \, (modn).$$

Observing that $0 \times t, 1 \times t, 2 \times t, \ldots, (n-1) \times t$ in the Eq (4.4) is just a reordering of $0, 1, 2, \ldots, n-1$, we see that $a_{k_0} a_{k_1} a_{k_2} \ldots a_{k_{n-1}}$ is also one term in b_j.

Conversely, it is also easy to see that every term $a_{k_0} a_{k_1} a_{k_2} \ldots a_{k_{n-1}}$ with $0 \leq k_s \leq n-1$ in b_j is a one term in b_i. Thus, claim **1** is true.

Next, we claim the following:

Claim 2. $\Delta = b_0 - b_1$.

In fact, by Claim 1, we have $b_1 \varepsilon + \cdots + b_i \varepsilon^i + \cdots + b_{n-1} \varepsilon^{n-1} = b_1(\varepsilon + \cdots + \varepsilon^i + \cdots + \varepsilon^{n-1})$. Noticing that $1, \varepsilon, \cdots, \varepsilon^i, \cdots, \varepsilon^{n-1}$ are all roots of $x^n = 1$, we see that $\varepsilon + \cdots + \varepsilon^i + \cdots + \varepsilon^{n-1} = -1$ by the relationship between roots and coefficients, therefore, $\Delta = b_0 - b_1$.

Now, we consider the computation of b_0 and b_1. By Eqs (4.1) and (4.3), we need to find all possible values $k_0, k_1, \ldots, k_{n-1}$ such that $i = 0$ or $i = 1$ in (4.1). Noticing that k_j is considered in the case of module n, we may assume $k_j \in Z_n = Z/\langle n \rangle$ for $0 \leq j \leq n-1$. Based on the above discussion, if $k_0, k_1, \ldots, k_{n-1}$ satisfy (4.1) for $i = 0$ or $i = 1$, then $k_0, k_1, \ldots, k_{n-1}$ must be a solution of the following systems of linear equations (4.5) for $i = 0$ or (F) for $i = 1$:

$$0 \times x_0 + 1 \times x_1 + 2 \times x_2 + \cdots + \cdots + (n-1) \times x_{n-1} \equiv 0. \tag{4.5}$$

or

$$0 \times x_0 + 1 \times x_1 + 2 \times x_2 + \cdots + \cdots + (n-1) \times x_{n-1} \equiv 1. \tag{4.6}$$

Conversely, every solution $k_0, k_1, \ldots, k_{n-1}$ of the systems (4.5) and (4.6) must satisfy (4.1) for either $i = 0$ or $i = 1$. Therefore, we should find all solutions of (4.5) and (4.6).

It is clear that (modulo n)

$$\begin{pmatrix}1\\0\\0\\0\\\vdots\\0\\\vdots\\0\end{pmatrix},\begin{pmatrix}0\\n-2\\1\\0\\\vdots\\0\\\vdots\\0\end{pmatrix},\begin{pmatrix}0\\n-3\\0\\1\\\vdots\\0\\\vdots\\0\end{pmatrix},\dots,\begin{pmatrix}0\\n-i\\0\\0\\\vdots\\1\\\vdots\\0\end{pmatrix},\dots,\begin{pmatrix}0\\1\\0\\0\\\vdots\\0\\\vdots\\1\end{pmatrix}$$

is a basic solution system of the systems of linear equation (4.5). Thus, the general solution of (4.5) is as follows:

$$\left[c_0\begin{pmatrix}1\\0\\0\\0\\\vdots\\0\\\vdots\\0\end{pmatrix}+c_2\begin{pmatrix}0\\n-2\\1\\0\\\vdots\\0\\\vdots\\0\end{pmatrix}+c_3\begin{pmatrix}0\\n-3\\0\\1\\\vdots\\0\\\vdots\\0\end{pmatrix}+\cdots+c_{n-1}\begin{pmatrix}0\\1\\0\\0\\\vdots\\0\\\vdots\\1\end{pmatrix}\right]$$

$$=\begin{pmatrix}c_0\\(n-2)c_2+(n-3)c_3+\cdots+(n-i)c_i+\cdots+c_{n-1}\\c_2\\c_3\\\vdots\\c_i\\\vdots\\c_{n-1}\end{pmatrix},$$

where $c_0, c_2, \cdots, c_{n-1}$ in Z_n are arbitrary.

It is also easy to see that

$$\begin{pmatrix}0\\1\\0\\0\\\vdots\\0\\\vdots\\0\end{pmatrix}$$

is a solution of the systems of linear equation (4.6). Thus, the general solution of the systems of linear equation (4.6) is as follows:

$$\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ \vdots \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \begin{pmatrix} c_0 \\ (n-2)c_2 + (n-3)c_3 + \cdots + (n-i)c_i + \cdots + c_{n-1} \\ c_2 \\ c_3 \\ \vdots \\ c_i \\ \vdots \\ c_{n-1} \end{pmatrix}$$

$$= \begin{pmatrix} c_0 \\ 1 + (n-2)c_2 + (n-3)c_3 + \cdots + (n-i)c_i + \cdots + c_{n-1} \\ c_2 \\ c_3 \\ \vdots \\ c_i \\ \vdots \\ c_{n-1} \end{pmatrix},$$

where $c_0, c_2, \cdots, c_{n-1}$ in Z_n are arbitrary.

Hence

$$b_0 = \sum_{c_0, c_2, \ldots, c_i, \ldots, c_{n-1}} a_{c_0} a_{[(n-2)c_2 + (n-3)c_3 + \cdots + c_{n-1}](mod n)} a_{c_2} a_{c_3} \ldots a_{c_i} \ldots a_{c_{n-1}},$$

and

$$b_1 = \sum_{c_0, c_2, \ldots, c_i, \ldots, c_{n-1}} a_{c_0} a_{[1 + (n-2)c_2 + (n-3)c_3 + \cdots + c_{n-1}](mod n)} a_{c_2} a_{c_3} \ldots a_{c_i} \ldots a_{c_{n-1}},$$

where $c_0, c_2, \ldots, c_i, \ldots, c_{n-1}$ satisfies $0 \le c_r \le n-1$ for $r \in \{0, 2, \ldots, n-1\}$.

For convenience, let $\Phi = [(n-2)c_2 + (n-3)c_3 + \cdots + c_{n-1}](mod n)$. Then,

$$\begin{aligned} \Delta &= b_0 - b_1 \\ &= \sum_{\Phi=0} a_{c_0}(a_0 - a_1) a_{c_2} a_{c_3} \ldots a_{c_{n-1}} \\ &+ \sum_{\Phi=1} a_{c_0}(a_1 - a_2) a_{c_2} a_{c_3} \ldots a_{c_{n-1}} \\ &+ \cdots \\ &+ \sum_{\Phi=n-2} a_{c_0}(a_{n-2} - a_{n-1}) a_{c_2} a_{c_3} \ldots a_{c_{n-1}} \end{aligned}$$

$$+ \sum_{\Phi=n-1} a_{c_0}(a_{n-1} - a_0)a_{c_2}a_{c_3}\dots a_{c_{n-1}}$$

$$= \sum_{k=0}^{n-2} \sum_{\Phi=k} a_{c_0}(a_k - a_{k+1})a_{c_2}a_{c_3}\dots a_{c_{n-1}}$$

$$+ \sum_{\Phi=n-1} a_{c_0}(a_{n-1} - a_0)a_{c_2}a_{c_3}\dots a_{c_{n-1}}.$$

Now, we can state the following results.

Theorem 4.1. Let $a_0, a_1, \cdots, a_{n-1}$ be real nubers and let $A = Circ(a_0, a_1, \cdots, a_{n-1})$ be the corresponding circulant matrix with a prime n. If Δ is the determinant of A, then

$$\Delta = \sum_{k=0}^{n-2} \sum_{\Phi=k} a_{c_0}(a_k - a_{k+1})a_{c_2}a_{c_3}\dots a_{c_{n-1}}$$

$$+ \sum_{\Phi=n-1} a_{c_0}(a_{n-1} - a_0)a_{c_2}a_{c_3}\dots a_{c_{n-1}}.$$

where $c_0, c_2, \dots, c_{n-1}$ satisfy $0 \le c_r \le n-1$ for $r \in \{0, 2, \dots, n-1\}$ and $\Phi = [(n-2)c_2 + (n-3)c_3 + \cdots + c_{n-1}](modn)$.

Since a matrix A is invertible if and only if its determinant $|A| \neq 0$, Theorem 4.1 can provide a necessary and sufficient condition for the invertibility of circulant matrices with a prime order.

5. Examples

In this section, we provide two examples to explain how to use the obtained results to calculate the determinant of a circulant matrix.

Example 5.1. Let $A_1 = Circ(0, 1, 2, 3, 4, 5, 6)$. Then, by Theorem 3.1, A_1 is invertible. Since the arrangement of A_1 is simple, it is easy to calculate the determinant of A_1 by using the properties of the determinant. On the other hand, we can use Theorem 4.1 to calculate the determinant of A_1 by Matlab, where $|A_1| = 352947$. The actual implementation (code) can be found in Figure 1.

Example 5.2. Let $A_2 = Circ(0, 1, 3, 4, 6, 8, 9)$. Then, by Theorem 3.1, A_2 is invertible. By Theorem 4.1, we can calculate the determinant of A_2 by Matlab, where $|A_2| = 5843624$. The actual implementation (code) can be found in Figure 1.

```
function [x,time]=function1(a,b,c,d,e,f,g)
H=[a,b,c,d,e,f,g];
x=0;
c0=0:1:6;
c1=0:1:6;
c2=0:1:6;
c3=0:1:6;
c4=0:1:6;
c5=0:1:6;

tic;
for t=1:7
   for i=1:7
      for j=1:7
         for s=1:7
            for r=1:7
               for k=1:7
               p=5*c1(i)+4*c2(j)+ 3*c3(s)+2*c4(r)+c5(k);
               if mod(p,7)<= 5
                  x=x + H(t)*(H(mod(p,7) + 1)-H(mod(p,7)+ 2))*H(i)*H(j)*H(s)*H(r)*H(k);
               else
                  x=x + H(t)*(H(mod(p,7) + 1) - H(1))*H(i)*H(j)*H(s)*H(r)*H(k);
               end
               end
            end
         end
      end
   end
end
time = toc;

[x,time]=function1(0,1,2,3,4,5,6)  result: x=352947,  time=0.0858

[x,time]=function1(0,1,3,4,6,8,9)  result: x=5843624,  time=0.0325
```

Figure 1. Our algorithm.

Remark 5.3. Theorem 4.1 greatly simplifies the calculation of the determinant of a circulant matrix with a prime order. For example, let $f_1(x) = x + 2x^2 + 3x^3 + 4x^4 + 5x^5 + 6x^6$ and $f_2(x) = x + 3x^2 + 4x^3 + 6x^4 + 8x^5 + 9x^6$. By Lemma 2.1, $|A_1| = \Pi_{j=0}^{6} f_1(\varepsilon^j)$ and $|A_2| = \Pi_{j=0}^{6} f_2(\varepsilon^j)$, where ε is a primitive 7-th root of unity, and A_1 and A_2 are exactly A_1 in Example 5.1 and A_2 in Example 5.2. If we calculate $\Pi_{j=0}^{6} f_1(\varepsilon^j)$ and $\Pi_{j=0}^{6} f_2(\varepsilon^j)$ by Matlab, the required calculation times are 0.3688 seconds and 0.2488 seconds, respectively (see Figure 2), and the required number of calculations is $7^8 + 7 \times 28$ times. However, if we calculate $|A_1|$ and $|A_2|$ by Matlab (using Theorem 4.1), then the required calculation times are 0.0858 seconds and 0.0325 seconds, respectively (see Figure 1), and the required number of calculations is $7^6 \times 18$ times.

```
function [x,time]=function2(a,b,c,d,e,f,g)

H=[a,b,c,d,e,f,g];

p = [1, 0, 0, 0, 0, 0, 0, -1];
roots_of_poly = roots(p);

H1=[a,b* roots_of_poly(1),c* roots_of_poly(1)^2,d* roots_of_poly(1)^3, e*roots_of_poly(1)^4,f* roots_of_poly(1)^5,g* roots_of_poly(1)^6];
H2=[a,b* roots_of_poly(2),c* roots_of_poly(2)^2,d* roots_of_poly(2)^3,e* roots_of_poly(2)^4,f* roots_of_poly(2)^5,g* roots_of_poly(2)^6];
H3=[a,b* roots_of_poly(3),c* roots_of_poly(3)^2,d* roots_of_poly(3)^3, e*roots_of_poly(3)^4,f* roots_of_poly(3)^5,g* roots_of_poly(3)^6];
H4=[a,b* roots_of_poly(4),c* roots_of_poly(4)^2,d* roots_of_poly(4)^3,e* roots_of_poly(4)^4,f* roots_of_poly(4)^5,g* roots_of_poly(4)^6];
H5=[a,b* roots_of_poly(5),c* roots_of_poly(5)^2,d* roots_of_poly(5)^3, e*roots_of_poly(5)^4,f* roots_of_poly(5)^5,g* roots_of_poly(5)^6];
H6=[a,b* roots_of_poly(6),c* roots_of_poly(6)^2,d* roots_of_poly(6)^3,e* roots_of_poly(6)^4,f* roots_of_poly(6)^5,g* roots_of_poly(6)^6];
H7=[a,b* roots_of_poly(7),c* roots_of_poly(7)^2,d* roots_of_poly(7)^3, e*roots_of_poly(7)^4,f* roots_of_poly(7)^5,g* roots_of_poly(7)^6];

x=0;

tic;
for t=1:7
    for i=1:7
        for j=1:7
            for s=1:7
                for r=1:7
                    for k=1:7
                        for u=1:7
                        x=x+H1(t)*H2(i)*H3(j)*H4(s)*H5(r)*H6(k)*H7(u);
                        end
                    end
                end
            end
        end
    end
end
time=toc;

x = round(abs(x));

[x,time]=function2(0,1,2,3,4,5,6)  result: x=352947, time=0.3688

[x,time]=function2(0,1,3,4,6,8,9)  result: x=5843624, time=0.2408
```

Figure 2. Original algorithm.

Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

The authors would like to thank the referees for their valuable suggestions and useful comments contributed to the final version of this paper. The authors also would like to express gratitude to Professor Wanzhou Ye and Professor Pengfei Bai for their assistance in preparing the manuscript. The first author was supported by the National Natural Science Foundation of China (12171302).

Conflict of interest

The authors declare there is no conflicts of interest.

References

1. I. B. Collings, I. Vaughan, L. Clarkson, A low-complexity lattice-based low-PAR transmission scheme for DSL channels, *IEEE Trans. Commun.*, **52** (2004), 755–764. https://doi.org/10.1109/TCOMM.2004.826261
2. P. J. Davis, *Circulant Matrices*, 2^{nd} edition, Chelsea Publishing, New York, 1994.
3. B. Gellai, Determination of molecular symmetry coordinates using circulant matrices, *J Mol. Struct.*, **1** (1984), 21–26. https://doi.org/10.1016/S0022-2860(84)87196-3
4. A. Carmona, A. M. Encinas, S. Gagoa, M. J. Jiménez, M. Mitjana, The inverses of some circulant matrices, *Appl. Math. Comput.*, **270** (2015), 785–793. https://doi.org/10.1016/j.amc.2015.08.084
5. F. Lin, The inverse of circulant matrix, *Appl. Math. Comput.*, **217** (2011), 8495–8503. https://doi.org/10.1016/j.amc.2011.03.052
6. O. Rojo, H. Rojo, Some results on symmetric circulant matrices and on symmetric centrosymmetric matrices, *Linear Algebra Appl.*, **392** (2004), 211–233. https://doi.org/10.1016/j.laa.2004.06.013
7. S. Q. Shen, J. M. Cen, Y. Hao, On the determinants and inverses of circulant matrices with fibonacci and lucas numbers, *Appl. Math. Comput.*, **217** (2011), 9790–9797. https://doi.org/10.1016/j.amc.2011.04.072
8. R. M. Gray, Toeplitz and circulant matrices: A review,, *Found. Trends Commun. Inf. Theory*, **2** (2006), 155–239. http://doi.org/10.1561/0100000006
9. M. N. Huxley, M. C. Lettington, K. M. Schmidt, On the structure of additive systems of integers, *Period. Math. Hung.*, **78** (2019), 178–199. http://doi.org/10.1007/s10998-018-00275-w
10. M. C. Lettington, K. M. Schmidt, Divisor functions and the number of sum systems, *Integers*, preprint, arXiv:1910.02455. https://doi.org/10.48550/arXiv.1910.02455
11. M. C. Lettington, K. M. Schmidt, On the sum of left and right circulant matrices, *Linear Algebra Appl.*, **658** (2023), 62–85. https://doi.org/ 10.1016/j.laa.2022.10.024