Bull. Korean Math. Soc. **40** (2003), No. 3, pp. 425–435

EFFICIENT ALGORITHMS FOR COMPUTING THE MINIMAL POLYNOMIALS AND THE INVERSES OF LEVEL-k Π-CIRCULANT MATRICES

ZHAOLIN JIANG AND SANYANG LIU

ABSTRACT. In this paper, a new kind of matrices, i.e., level-k Π-circulant matrices is considered. Algorithms for computing minimal polynomial of this kind of matrices are presented by means of the algorithm for the Gröbner basis of the ideal in the polynomial ring. Two algorithms for finding the inverses of such matrices are also presented based on the Buchberger's algorithm.

0. Introduction

Circulant matrices, as an important class of special matrices, have a wide range of interesting applications in numerical computation, signal processing, coding theory and oil investigation, and so on. In this paper, a new kind of circulant matrices, level-k Π-circulant matrices over a field, is introduced.

The minimal polynomial of a matrix has a wide range of applications in the decomposition of a vector space and the diagonalization of a matrix. But it is not easy to find a minimal polynomial of a given matrix. In this paper, an algorithm for computing the minimal polynomials of such matrices is given by means of the algorithm for Gröbner basis of an ideal, which can be realized by CoCoA 4.0, a system of Algebra, in the field of rational numbers or in the ring of residue classes of modulo a given prime number.

We show that the ring of all level-k Π-circulant matrices over a field is isomorphic to a factor ring of a polynomial ring in k variables over the same field and then present an algorithm for the minimal polynomial of a level-k Π-circulant matrix by mean of the algorithm for the Gröbner

Received January 25, 2002.
2000 Mathematics Subject Classification: 15A21, 65F15.
Key words and phrases: Gröbner basis, minimal polynomial, level-k Π-circulant matrix, inverse.

basis for a kernel of a ring homomorphism. We also give a sufficient and necessary condition to determine whether a level-k Π-circulant matrix over a field is singular or not and then present two algorithm for the inverse of a level-k Π-circulant matrix over a field.

We give now some terminologies and notation here. Let $\mathbb{F}$ be a field and $\mathbb{F}[x_1, \ldots, x_k]$ the polynomial ring in k variables over the field $\mathbb{F}$. By Hilbert Basis Theorem, we know that every ideal $\mathbf{I}$ in $\mathbb{F}[x_1, \ldots, x_k]$ is finitely generated. Fixing a term order in $\mathbb{F}[x_1, \ldots, x_k]$, a set of non-zero polynomials $\mathbf{G} = \{g_1, \ldots, g_t\}$ in an ideal $\mathbf{I}$ is called a Gröbner basis for $\mathbf{I}$ if and only if for all non-zero $f \in \mathbf{I}$, there exists $i \in \{1, \ldots, t\}$ such that $lp(g_i)$ divides $lp(f)$, where $lp(g_i)$ and $lp(f)$ are the leading power products of g_i and f, respectively. A Gröbner basis $\mathbf{G} = \{g_1, \ldots, g_t\}$ is called a reduced Gröbner basis if and only if, for all i, $lc(g_i) = 1$ and g_i is reduced with respect to $\mathbf{G} - \{g_i\}$, that is, for all i, no non-zero term in g_i is divisible by any $lp(g_j)$ for any $j \neq i$, where $lc(g_i)$ is the leading coefficient of g_i.

In this paper, we set $A^0 = I$ for any square matrix A, and $\langle f_1, \ldots, f_m \rangle$ denotes an ideal of $\mathbb{F}[x_1, \ldots, x_k]$ generated by polynomials $f_1, \ldots, f_m$.

1. Definition and lemma

DEFINITION 1. An $n \times n$ matrix P over $\mathbb{F}$ is called a *permutation matrix* if exactly one entry in each row and column is equal to 1, and all other entries are 0.

DEFINITION 2. An $n \times n$ permutation matrix P over $\mathbb{F}$ is called a *basic circulant permutation matrix* if and only if

$$P^n = I_n, \tag{1}$$

where I_n is an $n \times n$ identity matrix, n is the smallest positive integer which satisfies the above equation (1).

Obviously, the minimal polynomial of an $n \times n$ basic circulant permutation matrix P is $x^n - 1$. In the following

Let P_i be an $n_i \times n_i$ basic circulant permutation matrix and $\Pi = (P_1, P_2, \ldots, P_k)$.

Let I_{n_i} be the $n_i \times n_i$ identity matrix for $i = 1, 2, \ldots, k$ and $N = n_1 n_2 \ldots n_k$. Set

$$\sigma_i = I_{n_1} \otimes \cdots \otimes I_{n_{i-1}} \otimes P_i \otimes I_{n_{i+1}} \otimes \cdots \otimes I_{n_k}$$

for $i = 1, 2, \ldots, k$, where $\otimes$ is a Kronecker product of matrices.

DEFINITION 3. An $N \times N$ matrix A over $\mathbb{F}$ is called a *level-k Π-circulant matrix* if there exists $f(x_1, x_2, \ldots, x_k) = \sum_{i_1=0}^{n_1-1} \cdots \sum_{i_k=0}^{n_k-1} a_{i_1 \ldots i_k} x_1^{i_1} \ldots x_k^{i_k} \in \mathbb{F}[x_1, \ldots, x_k]$ such that

$$A = f(\sigma_1, \ldots, \sigma_k) = \sum_{i_1=0}^{n_1-1} \cdots \sum_{i_k=0}^{n_k-1} a_{i_1 \ldots i_k} \sigma_1^{i_1} \ldots \sigma_k^{i_k},$$

where the polynomial $f(x_1, x_2, \ldots, x_k)$ is called an *adjoint polynomial* of A.

By the above representation, we know that level-k Π-circulant matrices have very nice structure, which can be related to P_i. Since $P_i^{n_i} = I_{n_i}$, the product of two level-k Π-circulant matrices is a level-k Π-circulant matrix. Furthermore, level-k Π-circulant matrices commute under multiplication and A^{-1} is also a level-k Π-circulant matrix. Let

$$\mathbb{F}[\sigma_1, \ldots, \sigma_k] = \{A | A = f(\sigma_1, \ldots, \sigma_k), f(x_1, \ldots, x_k) \in \mathbb{F}[x_1, \ldots, x_k]\}.$$

It is a routine to prove that $\mathbb{F}[\sigma_1, \ldots, \sigma_k]$ is a commutative ring with the matrix addition and multiplication.

DEFINITION 4. Let $\mathbf{I}$ be a non-zero ideal of the polynomial ring $\mathbb{F}[y_1, \ldots, y_t]$. Then $\mathbf{I}$ is called an *annihilation ideal* of square matrices $A_1, \ldots, A_t$, denoted by $\mathbf{I}(A_1, \ldots, A_t)$, if $f(A_1, \ldots, A_t) = 0$ for all $f(y_1, \ldots, y_t) \in \mathbf{I}$.

DEFINITION 5. Suppose that $A_1, \ldots, A_t$ are not all zero matrices. The unique monic polynomial $p(x)$ of minimum degree that simultaneously annihilates $A_1, \ldots, A_t$ is called the *common minimal polynomial* of $A_1, \ldots, A_t$.

We give the special case of [1, Theorem 2.4.10] here for the convenience of applications.

LEMMA 1. *Let $\mathbf{I}$ be an ideal of $\mathbb{F}[x_1, \ldots, x_k]$. Given $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_k]$, consider the following $\mathbb{F}$-algebra homomorphism*

$$\begin{array}{rcl} \varphi : \mathbb{F}[y_1, \ldots, y_m] & \to & \mathbb{F}[x_1, \ldots, x_k]/\mathbf{I} \\ y_1 & \mapsto & f_1 + \mathbf{I} \\ \ldots & \ldots & \ldots \\ y_m & \mapsto & f_m + \mathbf{I} \end{array}$$

Let $\mathbf{K} = \langle \mathbf{I}, y_1 - f_1, \ldots, y_m - f_m \rangle$ be an ideal of $\mathbb{F}[x_1, \ldots, x_k, y_1, \ldots, y_m]$ generated by $\mathbf{I}, y_1 - f_1, \ldots, y_m - f_m$. Then $\ker\varphi = \mathbf{K} \cap \mathbb{F}[y_1, \ldots, y_m]$.

LEMMA 2. $\mathbb{F}[x_1, \ldots, x_k]/\langle x_1^{n_1} - 1, \ldots, x_k^{n_k} - 1 \rangle \cong \mathbb{F}[\sigma_1, \ldots, \sigma_k]$.

Proof. Consider the following $\mathbb{F}$-algebra homomorphism

$$\begin{aligned} \varphi : \mathbb{F}[x_1, \ldots, x_k] &\to \mathbb{F}[\sigma_1, \ldots, \sigma_k] \\ f(x_1, \ldots, x_k) &\mapsto A = f(\sigma_1, \ldots, \sigma_k) \end{aligned}$$

for $f(x_1, \ldots, x_k) \in \mathbb{F}[x_1, \ldots, x_k]$. It is clear that φ is an $\mathbb{F}$-algebra epimorphism. So we have

$$\varphi : \mathbb{F}[x_1, \ldots, x_k]/ker\varphi \cong \mathbb{F}[\sigma_1, \ldots, \sigma_k].$$

We prove that $\ker\varphi = \langle x_1^{n_1} - 1, x_2^{n_2} - 1, \ldots, x_k^{n_k} - 1\rangle$ as following.

Since $\sigma_i^{n_i} - I_{n_i} = 0$ for $i = 1, 2, \ldots, k$, then $x_i^{n_i} - 1 \in \ker\varphi$ for $i = 1, 2, \ldots, k$. Hence $\ker\varphi \supseteq \langle x_1^{n_1} - 1, x_2^{n_2} - 1, \ldots, x_k^{n_k} - 1\rangle$.

For any $f(x_1, \ldots, x_k) \in \mathbb{F}[x_1, \ldots, x_k]$, we have $A = f(\sigma_1, \ldots, \sigma_k) = 0$. Fix the lexicographical order on $\mathbb{F}[x_1, \ldots, x_k]$ with $x_1 > x_2 > \cdots > x_k$. $x_1^{n_1} - 1$ dividing $f(x_1, \ldots, x_k)$, there exist $u_1(x_1, \ldots, x_k), v_1(x_1, \ldots, x_k) \in \mathbb{F}[x_1, \ldots, x_k]$ such that

$$f(x_1, \ldots, x_k) = u_1(x_1, \ldots, x_k)(x_1^{n_1} - 1) + v_1(x_1, \ldots, x_k),$$

where $v_1(x_1, \ldots, x_k) = 0$ or the largest degree of x_1 in $v_1(x_1, \ldots, x_k)$ is less than n_1.

If $v_1(x_1, \ldots, x_k) = 0$, then $f(x_1, \ldots, x_k) \in \langle x_1^{n_1} - 1, x_2^{n_2} - 1, \ldots, x_k^{n_k} - 1\rangle$. Otherwise, $x_2^{n_2} - 1$ dividing $v_1(x_1, \ldots, x_k)$, there exist $u_2(x_1, \ldots, x_k)$, $v_2(x_1, \ldots, x_k) \in \mathbb{F}[x_1, \ldots, x_k]$ such that

$$v_1(x_1, \ldots, x_k) = u_2(x_1, \ldots, x_k)(x_2^{n_2} - 1) + v_2(x_1, \ldots, x_k),$$

where $v_2(x_1, \ldots, x_k) = 0$ or the largest degree of x_2 in $v_2(x_1, \ldots, x_k)$ is less than n_2. If $v_2(x_1, \ldots, x_k) = 0$, then $f(x_1, \ldots, x_k) \in \langle x_1^{n_1} - 1, x_2^{n_2} - 1, \ldots, x_k^{n_k} - 1\rangle$. Otherwise, if $v_2(x_1, \ldots, x_k) \neq 0$, the largest degree of x_1 in $v_2(x_1, \ldots, x_k)$ is less than n_1 because x_1 does not appear in $x_2^{n_2} - 1, x_3^{n_3} - 1$ dividing $v_2(x_1, \ldots, x_k)$, there exist $u_3(x_1, \ldots, x_k), v_3(x_1, \ldots, x_k) \in \mathbb{F}[x_1, \ldots, x_k]$ such that

$$v_2(x_1, \ldots, x_k) = u_3(x_1, \ldots, x_k)(x_3^{n_3} - 1) + v_3(x_1, \ldots, x_k),$$

where $v_3(x_1, \ldots, x_k) = 0$ or the largest degree of x_3 in $v_3(x_1, \ldots, x_k)$ is less than n_3. If $v_3(x_1, \ldots, x_k) = 0$, then $f(x_1, \ldots, x_k) \in \langle x_1^{n_1} - 1, x_2^{n_2} - 1, \ldots, x_k^{n_k} - 1\rangle$. Otherwise, if $v_3(x_1, \ldots, x_k) \neq 0$, the largest degrees of x_1 and x_2 in $v_3(x_1, \ldots, x_k)$ are less than n_1 and n_2, respectively, because x_1 and x_2 do not appear in $x_3^{n_3} - 1$. Continuing this procedure, there exist $u_1(x_1, \ldots, x_k), u_2(x_1, \ldots, x_k), \ldots, u_k(x_1, \ldots, x_k), v_k(x_1, \ldots, x_k) \in \mathbb{F}[x_1, \ldots, x_k]$ such that

$$\begin{aligned} f(x_1, \ldots, x_k) = {} & u_1(x_1, \ldots, x_k)(x_1^{n_1} - 1) + \cdots \\ & + u_k(x_1, \ldots, x_k)(x_k^{n_k} - 1) + v_k(x_1, \ldots, x_k), \end{aligned}$$

where $v_k(x_1,\ldots,x_k)=0$ or the degrees of $x_1,x_2,\ldots,x_k$ in $v_k(x_1,\ldots,x_k)$ are less than $n_1,n_2,\ldots,n_k$, respectively. If $v_k(x_1,\ldots,x_k)=0$, then

$$f(x_1,\ldots,x_k)\in\langle x_1^{n_1}-1,x_2^{n_2}-1,\ldots,x_k^{n_k}-1\rangle.$$

Suppose that $v_k(x_1,\ldots,x_k)\neq 0$, then $v_k(\sigma_1,\ldots,\sigma_k)=0$, because $f(\sigma_1,\ldots,\sigma_k)=0$ and $\sigma_i^{n_i}-I_{n_i}=0$ for all $i=1,2,\ldots,k$. Since the degrees of $x_1,x_2,\ldots,x_k$ in $v_k(x_1,\ldots,x_k)$ are less than $n_1,n_2,\ldots,n_k$, respectively, the coefficients of all terms in $v_k(x_1,\ldots,x_k)$ are the entries of the matrix $v_k(\sigma_1,\ldots,\sigma_k)$. Therefore each coefficient of each term in $v_k(x_1,\ldots,x_k)$ is 0, i.e. $v_k(x_1,\ldots,x_k)$=0. This occurs a contradiction to $v_k(x_1,\ldots,x_k)\neq 0$.

The following lemma is well known [2].

LEMMA 3. *Let A be a non-zero matrix over $\mathbb{F}$, if the minimal polynomial of A is:*

$$p(y)=a_0y^n+a_1y^{n-1}+a_2y^{n-2}+\cdots+a_n$$

and $a_n\neq 0$, then $A^{-1}=(1/a_n)(-a_0A^{n-1}-a_1A^{n-2}-\cdots-a_{n-1}I)$.

The following Lemma is the Exercise 2.38 of [1].

LEMMA 4. *Let $\mathbf{L}_1,\mathbf{L}_2,\ldots,\mathbf{L}_m$ be ideals of $\mathbb{F}[x_1,x_2,\ldots,x_k]$ and let $\mathbf{J}=\langle 1-\sum_{i=1}^m w_i, w_1\mathbf{L}_1,w_2\mathbf{L}_2,\ldots,w_m\mathbf{L}_m\rangle$ be an ideal of $\mathbb{F}[x_1,x_2,\ldots,x_k,w_1,\ldots,w_m]$ generated by $1-\sum_{i=1}^m w_i,w_1\mathbf{L}_1,w_2\mathbf{L}_2,\ldots,w_m\mathbf{L}_m$. Then $\bigcap_{i=1}^m\mathbf{L}_i=\mathbf{J}\bigcap\mathbb{F}[x_1,x_2,\ldots,x_k]$.*

2. Main results and proof

In the section, the algorithm for the minimal polynomial and two algorithm for the inverse of level-k Π-circulant matrix is given here. By the Lemma 2, we can prove the following Theorem

THEOREM 1. *The minimal polynomial of the level-k Π-circulant matrix $A\in\mathbb{F}[\sigma_1,\ldots,\sigma_k]$ is the monic polynomial that generates the ideal*

$$\langle x_1^{n_1}-1,\ldots,x_k^{n_k}-1,y-f(x_1,\ldots,x_k)\rangle\cap\mathbb{F}[y],$$

where the polynomial $f(x_1,\ldots,x_k)$ is an adjoint polynomial of A.

Proof. Consider the following $\mathbb{F}$-algebra homomorphism

$$\begin{aligned}\phi:\mathbb{F}[y] &\to \mathbb{F}[x_1,\ldots,x_k]/\langle x_1^{n_1}-1,\ldots,x_k^{n_k}-1\rangle\longrightarrow\mathbb{F}[\sigma_1,\ldots,\sigma_k]\\ y &\mapsto f(x_1,\ldots,x_k)+\langle x_1^{n_1}-1,\ldots,x_k^{n_k}-1\rangle\longmapsto A=f(\sigma_1,\ldots,\sigma_k).\end{aligned}$$

It is clear that $q(y) \in ker\phi$ if and only if $q(A) = 0$. By Lemma 1, we have

$$ker\phi = \langle x_1^{n_1} - 1, \ldots, x_k^{n_k} - 1, y - f(x_1, \ldots, x_k)\rangle \cap \mathbb{F}[y].$$

By Theorem 1 and Lemma 3, we know that the minimal polynomial and the inverse of a level-k Π-circulant matrix $A \in \mathbb{F}[\sigma_1, \ldots, \sigma_k]$ is calculated by a Gröbner basis for a kernel of an $\mathbb{F}$-algebra homomorphism. Therefore, we have the following algorithm to calculate the minimal polynomial and the inverse of a level-k Π-circulant matrix $A = f(\sigma_1, \ldots, \sigma_k)$:

Step 1. Calculate the reduced Gröbner basis $\mathbf{G}$ for the ideal

$$\langle x_1^{n_1} - 1, \ldots, x_k^{n_k} - 1, y - f(x_1, \ldots, x_k)\rangle \cap \mathbb{F}[y].$$

by CoCoA 4.0, using an elimination order with $x_1 > x_2 > \cdots > x_k > y$.

Step 2. Find the polynomial in $\mathbf{G}$ in which the variables $x_1, x_2, \ldots, x_k$ are not appear. This polynomial $p(y)$ is the minimal polynomial of A.

Step 3. By step 2, if a_n in the minimal polynomial of A

$$p(y) = a_0 y^n + a_1 y^{n-1} + a_2 y^{n-2} + \cdots + a_n$$

is zero, stop. Otherwise, calculate $A^{-1} = (1/a_n)(-a_0 A^{n-1} - a_1 A^{n-2} - \cdots - a_{n-1} I)$.

EXAMPLE 1. Let $A = f(\sigma_1, \sigma_2)$ be a level-2 Π-circulant matrix, where $f(x, y) = 2x^3y^2 + x^3y + 7x^2y^2 + 5x^3 + x^2y + 4x^2 + xy^2 + 9y^2 + 3xy + x + y + 1$. and $\sigma_1 = P_1 \otimes I_3, \sigma_2 = I_4 \otimes P_2$ and

$$P_1 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad P_2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

$$I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad I_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

We can now calculate the minimal polynomial and the inverse of A with coefficients in the field $\mathbf{Z}_{11}$ as following:

Program 1.

```
Use R::=Z/(11)[xyz], Lex;
Set Indentation;
```

I:=Ideal($x^4-1, y^3-1, z-2x^3y^2-x^3y-7x^2y^2-5x^3-x^2y-4x^2-xy^2-9y^2-3xy-x-y-1$);

ReducedGBasis(I);

By Program 1, we have the following reduced Gröbner basis for the ideal $\langle x^4-1, y^3-1, z-f(x,y)\rangle$:

$$[z^{12}-z^{11}-3z^{10}-2z^9-z^8-3z^7+4z^6-2z^5-4z^4+2z^3-3z^2+4z+4,$$
$$x+2z^{11}+5z^{10}+4z^9-5z^8-5z^7+z^6-5z^5-5z^4+4z^2+5z+2,$$
$$y-z^{11}+5z^{10}-5z^8+4z^7+4z^6+4z^4+4z^2+5z-5].$$

So the minimal polynomial of A is

$$z^{12}-z^{11}-3z^{10}-2z^9-z^8-3z^7+4z^6-2z^5-4z^4+2z^3-3z^2+4z+4.$$

Calculate the inverse of A

$$A^{-1}=(1/4)(-A^{11}+A^{10}+3A^9+2A^8+A^7+3A^6-4A^5+2A^4+4A^3-2A^2+3A-4I).$$

THEOREM 2. *The annihilation ideal of the level-k Π-circulant matrices $A_1,\ldots,A_t\in\mathbb{F}[\sigma_1,\ldots,\sigma_k]$ is*

$$\langle x_1^{n_1}-1,\ldots,x_k^{n_k}-1, y_1-f_1(x_1,\ldots,x_k),\ldots,y_t-f_t(x_1,\ldots,x_k)\rangle\cap\mathbb{F}[y_1,\ldots,y_t],$$

where the polynomial $f_i(x_1,\ldots,x_k)$ is an adjoint polynomial of $A_i, i=1,2,\ldots,t$.

Proof. Consider the following $\mathbb{F}$-algebra homomorphism

$$\begin{array}{rcl}\varphi:\mathbb{F}[y_1,\ldots,y_t] & \to & \mathbb{F}[x_1,\ldots,x_k]/\langle x_1^{n_1}-1,\ldots,x_k^{n_k}-1\rangle\longrightarrow\mathbb{F}[\sigma_1,\ldots,\sigma_k]\\ y_1 & \mapsto & f_1(x_1,\ldots,x_k)+\langle x_1^{n_1}-1,\ldots,x_k^{n_k}-1\rangle\longmapsto A_1=f_1(\sigma_1,\ldots,\sigma_k)\\ \ldots & \ldots & \ldots\ldots\ldots\ldots\ldots\ldots\\ y_t & \mapsto & f_t(x_1,\ldots,x_k)+\langle x_1^{n_1}-1,\ldots,x_k^{n_k}-1\rangle\longmapsto A_t=f_t(\sigma_1,\ldots,\sigma_k).\end{array}$$

It is clear that $\varphi(g(y_1,\ldots,y_t))=0$ if and only if $g(A_1,\ldots,A_t)=0$. So $I(A_1,\ldots,A_t)=\ker\varphi=\mathbf{J}\cap\mathbb{F}[y_1,\ldots,y_t]$, by Lemma 1.

According to Theorem 2, we give the following algorithm for the annihilation ideal of the level-k Π-circulant matrices :$A_1,\ldots,A_t\in\mathbb{F}[\sigma_1,\ldots,\sigma_k]$

Step 1. Calculate the reduced Gröbner basis $\mathbf{G}$ for the ideal

$$\langle x_1^{n_1}-1,\ldots,x_k^{n_k}-1, y_1-f_1(x_1,\ldots,x_k),\ldots,y_t-f_t(x_1,\ldots,x_k)\rangle$$

by CoCoA 4.0, using an elimination order with $x_1>\cdots>x_k>y_1>\cdots>y_k$.

Step 2. Find the polynomial in $\mathbf{G}$ in which the variables $x_1,x_2,\ldots,x_k$ are not appear. Then the ideal generated by these polynomials is the annihilation ideal of $A_1,\ldots,A_t$.

To calculate the common minimal polynomial of $A_1, \ldots, A_t$, we first prove the following Theorem. □

THEOREM 3. *Let $h(x)$ be the least common multiple of $p_1(x), p_2(x), \ldots, p_k(x)$. Then $\bigcap_{i=1}^{k} \langle p_i(x) \rangle = \langle h(x) \rangle$.*

Proof. For any $f(x) \in \bigcap_{i=1}^{k} \langle p_i(x) \rangle$, we have $p_i(x) \mid f(x)$ for $i = 1, 2, \ldots, k$. Since $h(x)$ is the least common multiple of $p_1(x), p_2(x), \ldots, p_k(x)$, $h(x) \mid f(x)$. So $f(x) \in \langle h(x) \rangle$. Hence $\bigcap_{i=1}^{k} \langle p_i(x) \rangle \subseteq \langle h(x) \rangle$.

Conversely, $p_i(x) \mid h(x)$ for $i = 1, 2, \ldots, k$. Because $h(x)$ is the least common multiple of $p_1(x), p_2(x), \ldots, p_k(x)$. So $\bigcap_{i=1}^{k} \langle p_i(x) \rangle \supseteq \langle h(x) \rangle$.

By Theorem 3 and Lemma 4, If the minimal polynomial of A_i is $p_i(x)$ for $i = 1, 2, \ldots, t$, then the common minimal polynomial of $A_1, \ldots, A_t$ is the least common multiple of $p_1(x)$, $p_2(x), \ldots, p_t(x)$. So we have the following algorithm for the common minimal polynomial of level-k Π-circulant matrices $A_i = f_i(\sigma_1, \ldots, \sigma_k)$ for $i = 1, 2, \ldots, t$:

Step 1. Calculate the Gröbner basis $\mathbf{G}_i$ for the ideal $\langle x_1^{n_1} - 1, \ldots, x_k^{n_k} - 1, y - f_i(x_1, \ldots, x_k) \rangle$ by CoCoA 4.0 for each $i = 1, 2, \ldots, t$, using an elimination order with $x_1 > \cdots > x_k > y$.

Step 2. Find out the polynomial $p_i(y)$ in $\mathbf{G}_i$ in which the variables $x_1, \ldots, x_k$ do not appear for each $i = 1, 2, \ldots, t$.

Step 3. Calculate the Gröbner basis $\mathbf{G}$ for the ideal $\langle 1 - \sum_{i=1}^{t} w_i, w_1 p_1(y), \ldots, w_t p_t(y) \rangle$ by CoCoA 4.0, using elimination with $w_1 > \cdots > w_t > y$.

Step 4. Find out the polynomial $p(y)$ in $\mathbf{G}$ in which the variables $w_1, \ldots, w_t$ do not appear. Then the polynomial $p(y)$ is the common minimal polynomial of $A_1, \ldots, A_t$. □

EXAMPLE 2. Let $A_1 = f_1(\sigma_1, \sigma_2)$ and $A_2 = f_2(\sigma_1, \sigma_2)$ be both level-2 Π-circulant matrices, where $\sigma_1 = P_1 \otimes I_4, \sigma_2 = I_4 \otimes P_2$,

$$f_1(x, y) = 3x^3y^3 + x^3y^2 + 4x^3y + 5x^3 + x^2y^3 + 6x^2y^2 + 5x^2y + x^2 + 3xy^3 + xy^2 + 2xy + x + 4y^3 + y^2 + y + 7,$$

$$f_2(x, y) = 2x^3y^3 + 5x^3y^2 + x^3y + 2x^3 + 7x^2y^3 + 4x^2y^2 + x^2y + 2x^2 + xy^3 + 7xy^2 + 3xy + 2x + y^3 + y^2 + 3y + 2,$$

and

$$P_1 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}, P_2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, I_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

We calculate the common minimal polynomial of A_1 and A_2 in the field $\mathbf{Z}_{11}$ as following:

Program 2.

Use R::=Z/(11)[xyz], Lex;

Set Indentation;

I:=Ideal($x^4-1, y^4-1, z-3x^3y^3-x^3y^2-4x^3y-5x^3-x^2y^3-6x^2y^2-5x^2y-x^2-3xy^3-xy^2-2xy-x-4y^3-y^2-y-7$);

ReducedGBasis(I);

By Program 2, we obtain the following reduced Gröbner basis for the ideal :

$\langle x^4-1, y^4-1, z-f_1(x,y)\rangle$

$[z^{14}+2z^{13}+3z^{12}+3z^{11}-2z^{10}-5z^9+5z^8-4z^7-z^6+4z^5-3z^4-3z^3-4z,$
$x-y+z^{13}+3z^{12}+2z^{11}-z^9+3z^8+2z^7+z^6-5z^5+3z^4-z^3-5z^2+2z-2,$
$y^3-y^2+y-5z^{13}-z^{12}+3z^{10}+5z^8+3z^7+z^5-4z^4+5z^3+5z^2+3z+3,$
$yz-2y+3z^{13}-2z^{12}-z^{11}-5z^{10}+z^8-5z^7+5z^6+3z^5-3z^4+5z^3-3z^2-4z-2]$

So the minimal polynomial $p_1(z)$ of A_1 is

$$z^{14}+2z^{13}+3z^{12}+3z^{11}-2z^{10}-5z^9+5z^8-4z^7-z^6+4z^5-3z^4-3z^3-4z.$$

Program 3.

Use R::=Z/(11)[xyz], Lex;

Set Indentation;

I:=Ideal($x^4-1, y^4-1, z-2x^3y^3-5x^3y^2-x^3y-2x^3-7x^2y^3-4x^2y^2-x^2y-2x^2-xy^3-7xy^2-3xy-2x-y^3-y^2-3y-2$);

ReducedGBasis(I);

By Program 3, we get the following reduced Gröbner basis for the ideal $\langle x^4-1, y^4-1, z-f_2(x,y)\rangle$:

$[z^{16}+z^{15}-z^{14}-5z^{13}-z^{12}-z^{11}-2z^{10}-4z^9+4z^8+5z^7+3z^6-z^5-3z^4$
$-5z^3+3z^2+3z,$
$x+5z^{13}-3z^{12}-2z^{11}+2z^{10}+3z^9+5z^8-4z^6-4z^5-z^4-z^2+5z-1,$
$y-4z^{15}+5z^{14}-5z^{13}+z^{12}-3z^{11}-4z^{10}-5z^9-5z^8-2z^7-5z^4+4z^3+2z^2-4z-1].$

So the minimal polynomial $p_2(z)$ of A_2 is

$$z^{16}+z^{15}-z^{14}-5z^{13}-z^{12}-z^{11}-2z^{10}-4z^9+4z^8$$
$$+5z^7+3z^6-z^5-3z^4-5z^3+3z^2+3z.$$

Program 4.

Use R::=Z/(11)[uvz], Lex;

Set Indentation;

I:=Ideal $(1-u-v, u(z^{14}+2z^{13}+3z^{12}+3z^{11}-2z^{10}-5z^9+5z^8-4z^7-z^6+4z^5-3z^4-3z^3-4z), v(z^{16}+z^{15}-z^{14}-5z^{13}-z^{12}-z^{11}-2z^{10}-4z^9+4z^8+5z^7+3z^6-z^5-3z^4-5z^3+3z^2+3z))$;

ReducedGBasis(I);

By Program 4, we obtain the following reduced Gröbner basis for the ideal $\langle 1-u-v, up_1(z), vp_2(z)\rangle$:

$$[u+v-1,$$
$$vz^4+5vz^3+3vz^2+4vz-z^{25}-4z^{24}+2z^{23}+3z^{22}+4z^{21}-z^{20}-4z^{19}+4z^{17}-5z^{16}$$
$$+4z^{15}+5z^{14}-2z^{13}+z^{12}+3z^{10}+z^9+z^8-5z^7-3z^6-z^5+4z^4+5z^3-2z^2+z,$$
$$z^{26}-2z^{25}+z^{23}+z^{22}-3z^{21}-z^{20}+z^{19}+3z^{18}+3z^{17}+z^{15}+5z^{13}$$
$$+2z^{12}-5z^{11}+3z^{10}-4z^9+3z^8-4z^6+4z^5+4z^4+5z^3+2z^2-3z].$$

So the common minimal polynomial $p(z)$ of A_1 and A_2 is

$$z^{26}-2z^{25}+z^{23}+z^{22}-3z^{21}-z^{20}+z^{19}+3z^{18}+3z^{17}+z^{15}+5z^{13}$$
$$+2z^{12}-5z^{11}+3z^{10}-4z^9+3z^8-4z^6+4z^5+4z^4+5z^3+2z^2-3z.$$

In the following, we discuss the singularity and the inverse of a level-k Π-circulant matrix.

THEOREM 4. *Let $A \in \mathbb{F}[\sigma_1,\ldots,\sigma_k]$ be an $N\times N$ level-k Π-circulant matrix. Then A is nonsingular if and only if $1 \in \langle f(x_1,\ldots,x_k), x_1^{n_1}-1,\ldots,x_k^{n_k}-1\rangle$, where the polynomial $f(x_1,\ldots,x_k)$ is an adjoint polynomial of A.*

Proof. A is nonsingular if and only if $f(x_1,\ldots,x_k)+\langle x_1^{n_1}-1,\ldots,x_k^{n_k}-1\rangle$ is an invertible element in $\mathbb{F}[x_1,\ldots,x_k]/\langle x_1^{n_1}-1,\ldots,x_k^{n_k}-1\rangle$.

By Lemma 2, if and only if there exists

$$g(x_1,\ldots,x_k)+\langle x_1^{n_1}-1,\ldots,x_k^{n_k}-1\rangle$$
$$\in \mathbb{F}[x_1,\ldots,x_k]/\langle x_1^{n_1}-1,\ldots,x_k^{n_k}-1\rangle$$

such that

$$f(x_1,\ldots,x_k)g(x_1,\ldots,x_k)+\langle x_1^{n_1}-1,\ldots,x_k^{n_k}-1\rangle$$
$$=1+\langle x_1^{n_1}-1,\ldots,x_k^{n_k}-1\rangle$$

if and only if there exist $g(x_1,\ldots,x_k), u_1(x_1,\ldots,x_k),\ldots,u_k(x_1,\ldots,x_k) \in \mathbb{F}[x_1,\ldots,x_k]$ such that

$$g(x_1,\ldots,x_k)f(x_1,\ldots,x_k)+u_1(x_1,\ldots,x_k)(x_1^{n_1}-1)$$
$$+\cdots+u_k(x_1,\ldots,x_k)(x_k^{n_k}-1)=1$$

if and only if $1 \in \langle f(x_1,\ldots,x_k), x_1^{n_1}-1,\ldots,x_k^{n_k}-1\rangle$. □

Let $A \in \mathbb{F}[\sigma_1,\ldots,\sigma_k]$ be an $N\times N$ level-k Π-circulant matrix, by Theorem 4, we have the following algorithm which can find the inverse of the matrix A:

Step 1. Calculate the reduced Gröbner basis $\mathbf{G}$ for the ideal

$$\langle f(x_1,\ldots,x_k), x_1^{n_1}-1,\ldots,x_k^{n_k}-1\rangle,$$

where the polynomial $f(x_1, \ldots, x_k)$ is an adjoint polynomial of A, by CoCoA 4.0, using a given term order with $x_1 > \cdots > x_k$. If $\mathbf{G} \neq \{1\}$, then A is singular. Stop. Otherwise, go to step 2.

Step 2. By Buchberger's algorithm for computing Gröbner bases, keeping track of linear combinations that give rise to the new polynomials in the generating set, we get $g(x_1, \ldots, x_k), u_1(x_1, \ldots, x_k), \ldots, u_k(x_1, \ldots, x_k) \in \mathbb{F}[x_1, \ldots, x_k]$ such that

$$g(x_1, \ldots, x_k) f(x_1, \ldots, x_k) + u_1(x_1, \ldots, x_k)(x_1^{n_1} - 1) + \cdots + u_k(x_1, \ldots, x_k)(x_k^{n_k} - 1) = 1.$$

Then $g(x_1, \ldots, x_k)$ is the adjoint polynomial of A^{-1}. We obtain $A^{-1} = g(\sigma_1, \ldots, \sigma_k)$.

References

[1] W. W. Adams and P. Loustaunau, *An introduction to Gröbner bases*, Amer. Math. Soc., 1994.

[2] D. Greenspan, *Methods of matrix inversion*, Amer. Math. Monthly. **62** (1955), 303–308.

[3] D. G. Northcott, *Injective envelopes and inverse polynomials*, J. London Math. Soc. **8** (1974), 190–196.

[4] H. M. Möller and F. Mora, *New constructive methods in classical ideal theory*, J. Algebra **100** (1986), 138–178.

[5] J. Zhaolin and Z. Zhangxin, *Circulant Matrices*, Chengdu: Chengdu Technology University Publishing Company, 1999.

[6] J. Baker, F. Hiergeist and G. Trapp, *The structure of multiblock circulants*, Kyungpook Math. J. **25** (1985), 71–75.

[7] TH. Chadjipantelis, STR. Kounias, and CHR. Moyssiadis, *Construction of D-optimal designs for N=2 mod 4 using block-circulant matrices*, J. Combin. Theory, Series A. **40** (1985), 125–135.

[8] B. Mishra, *Algorithmic Algebra*, Springer-Verlag, New York, 1993.

ZHAOLIN JIANG, DEPARTMENT OF APPLIED MATHEMATICS, XIDIAN UNIVERSITY, XI'AN, 710071, P. R. CHINA; DEPARTMENT OF MATHEMATICS, LINYI TEACHERS COLLEGE, LINYI 276005, SHANDONG, P. R. CHINA
E-mail: jzh1208@sina.com

SANYANG LIU, DEPARTMENT OF APPLIED MATHEMATICS, XIDIAN UNIVERSITY, XI'AN 710071, P. R. CHINA
E-mail: liusanyang@263.net