Journal of Mathematical Research and Exposition
Vol.10 No.1 Feb. 1990

Some Properties of Rational g-Circulant and Complexity of Inverting g-Circulant*

You Zhaoyong and Lu Hao

(Dept. Math. Xi'an Jiaotong University)

Abstract In this paper, it is shown that a rational g-circutant of order n can be diagonalized if $(g, n)=1$. Then, an algorithm with time conplexity $O(n \log n)$ is presented for inverse of g-circulant, where $(g.n)$ is the greatest common divisor of g and n.

I. Introduction

Let g be a non-negative integer, an $n\times n$ g-circulant matrix, or briefly an $n\times n$ g-circulant, $A=(a_{ij})$ is a matrix in which each row except the 0th row (the first row) is obtained from the previous row by shifting the entries cyclically g-columns to the right, i.e., $a_{ij}=a_{i-1,j-g}, i,j=0,1,\cdots,n-1$. where the indicies are reduced to their least non-negative remainders nodulo n. Some sufficient and necessary conditions for an $n\times n$ square matrix being a g-circulant were gi given by Davis [1]. Recently, it is shown that g-circulant can be diangonalized, if it is invertible[2].

In applications, for example, g-circulant can be used to solve the matrix equation $A^n=\lambda J+dI$[5−8] where B is integer or rational matrix, J is matrix with all entries being one. I is identity matrix. λ, d are constants. C.W.H. Lam[5] proved that $g\equiv 1 \pmod n$ if g-circulant A of order n is a solution of $B^n=dI+\lambda J$ $(d\neq 0)$. It is easy to see that $(g,n)=1$ if and only if there exist a positive integer m such that $g^n\equiv 1 \pmod n$. The purpose of this paper is to show that an $n\times n$ rational g-circulant can be diagonalized if $(g,n)=1$.

It is well known that strassen[9] algorithm for matrix multiplication can be used to inversion of matrix, that yields an algorithm with complexity $O(n^{2.871})$ for matrix inversion. The order of time complexity can be reduced fruther for some stronger structured matrices, such as 1-circulant, or circulant. Chen[3] showed that inverse of circulants can be computed in $O(n \log n)$ arithmetic operations as well as solution of circulant linear equations. In section 3, we will present an

* Received Apr. 18, 1988. This work was supported partly by the National Nalural Science Reundation of China.

© 1995-2005 Tsinghua Tongfang Optical Disc Co., Ltd. All rights reserved.

an algorithm for inverse of g-circulant. The dominant work of the algorithm is in performing the fast Fourier transform (FFT), therefore the time complexity is only $O(n\log n)$.

2. Preliminaries

For our purpose we need some elementary properties of g-circulant and permutation matrices as follows.

Proposition 2.1[1] Let R be the permutation matrix corresponding to the permutation

$$\begin{bmatrix} 0 & 1 & 2 & \cdots & 0 & \cdots & n-1 \\ 1 & 2 & 3 & \cdots & c+1 & \cdots & 0 \end{bmatrix} \tag{2.1}$$

Then the following result holds

$$R^{n+i} = R^i \quad (i = 0, 1, \cdots, n-1), \tag{2.2}$$

where $R^0 = I$

Proposition 2.2[1] An $n \times n$ matrix A is an $n \times n$ g-circulant if and only if

$$RA = AR^g \tag{2.3}$$

Proposition 2.3[1] An $n \times n$ matrix A is g-circulant with the first row $(a_0, a_1, \cdots, a_{n-1})$ if and only if

$$A = Q_g \sum_{i=0}^{n-1} a_1 R_1, \tag{2.4}$$

where Q is the g-circulant with the first row $(1, 0, \cdots, 0)$.

Proposition 2.4[1] Let A be circulant (1-circulant) with the first row $(a_0, a_1, \cdots, a_{n-1})$. Then

$$F^{-1}AF = \mathrm{diag}(\mu_2, \mu_2, \cdots, \mu_{n-1}), \tag{2.5}$$

where $F = (\omega_{ij})$ is the Fourier matrix of order n.

$$\mu_k = \sum_{i=0}^{n-1} a_i \omega^{ki} \quad (k = 0, 1, \cdots, n-1). \tag{2.6}$$

ω is the primitive nth roots of 1.

Proposition 2.5[2] Let P be a permutation matrix of order n. Then there exist positive integer m such that $P^m = I$.

Proposition 2.6[5] Product of a g-circulant with an h-circulant is a gh-circulant and inverse of a g-circulant is a g^{-1}-circulant, where gh and g^{-1} are taken nodulo n.

Proposition 2.7[2] An $n \times n$ g-circulant with the first row $(a_0, a_1, \cdots, a_{n-1})$ is invertible if and only if $(g, n) = 1$, $\mu_k = \sum_{i=0}^{n-1} a_i \omega^{ki} \neq 0$ $(k = 0, 1, \cdots, n-1)$.

3. Diagonalization of Rational g-Circulant

Theorem 3.1 A rational g-circulant is a diagonalization matrix, if $(n, g) = 1$.

© 1995-2005 Tsinghua Tongfang Optical Disc Co., Ltd. All rights reserved.

Proof If $g\equiv 1 \pmod n$, then A is circulant. The conclusion is immidiate from Proposition 2.4.

Otherwiss, since $(g,n)=1$, it is clear that Q_g is a permutation matrix. By Proposition 2.5, there exist a positive integer such that $Q_g^m=I$. Let $(a_0, a_1, \cdots, a_{n-1})$ be the first row of A, furthermore, applying Proposition 2.2 and 2.3, we obtain that

$$A^2=(Q_g\sum_{i=0}^{n-1}a_1R^1)(Q_g\sum_{j=0}^{n-1}a_jR^j)=Q_g^2\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}a_ia_jR^{ig+j}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$A^m=Q_g^n\sum_{i_1=0}^{n-1}\sum_{i_2=0}^{n-1}\cdots\sum_{i_m=0}^{n-1}a_1, a_{i2}\cdots a_{im}R^{i_1g^{m-1}+i_2g^{m-2}+\cdots+i_m}$$

$$=\sum_{i_1=0}^{n-1}\sum_{i_2=0}^{n-1}\cdots\sum_{i_m=0}^{n-1}a_{i1}a_{i2}\cdots a_{im}R^{i_1g^{m-1}+i_2g^{m-2}+\cdots+i_m} \qquad (3.1)$$

(3.1) implies that A^m is circulant, which can be diagonalized by the Fourier matrix, i.e.

$$F^{-1}A^mF=\operatorname{diag}(\lambda_0, \lambda_1, \cdots, \lambda_{n-1}) \qquad (3.2)$$

where

$$\lambda_k=\sum_{i_1=0}^{n-1}\sum_{i_2=0}^{n-1}\cdots\sum_{i_m=0}^{n-1}a_{i1}a_{i2}\cdots a_{im}\omega^{k(i_1g^{m-1}+i_2g^{m-2}+\cdots+i_m)} \qquad (k=0,1,\cdots n-1)$$

Assume that $\beta_1, \beta_2, \cdots, \beta_n$ are distinguish eigenvalues of A^m, diagonalization of A^m implies that the minimal polynomial of A^m must be

$$g(x)=(x-\beta_1)(x-\beta_2)\cdots(x-\beta_n) \qquad (3.3)$$

Let

$$J=\begin{bmatrix} J & & \\ & J_2 & \\ & & \ddots \\ & & & J_g \end{bmatrix} \qquad (3.4)$$

be the Jordan form of A, where J_i's are Jordan blocks of A. It is easy to see that A^m, J^m have the same minimal polynomial, and therefore

$$g(J^m)=0 \qquad (3.5)$$

(3.5) implies that the order of block corresponding to non-zero eigenvalue is one.

On other hand, from (2.1), we have

$$A^m=B_1B_2\cdots B_m \qquad (3.6)$$

$$A=Q_gB_m \qquad (3.7)$$

where

$$B_i=\sum_{j=0}^{n-1}a_jR^{jg^{m-i}} \quad (i=1,2,\cdots,m). \qquad (3.8)$$

B_i's are also diagonalized by Fourier matrix F, i.e.

© 1995-2005 Tsinghua Tongfang Optical Disc Co., Ltd. All rights reserved.

$$F^{-1}B_iF=\mathrm{diag}(\lambda_{i0},\lambda_{i1},\cdots,\lambda_{in-1}),\quad (i=1,2,\cdots,m)$$

where

$$\lambda_{ik}=\sum_{j=0}^{n-1} a_j\omega^{kjg^{m-i}} \quad (i=1,2,\cdots,m)$$
$$k=0,1,\cdots,n-1$$

Clearly, the eigenvalues λ_i's of A^m is given by the formula as follows

$$\lambda_i=\lambda_{1i}\lambda_{2i}\cdots\lambda_{ni} \quad (i=0,1,\cdots,n-1) \tag{3.10}$$

Let $f(x)=\sum_{j=0}^{n-1}a_ix^i$ and $h_a(x-\xi_1)(x-\xi_2)\cdots(x-\xi_t)$ be the cyclotomic polynomial Where ξ_i's are the primitive dth roots of 1, it is wel l known that each cycloto mic polynomial is irreduciale over the rationals. Hence, we have $h_a(x)\,|f(x)$, or $(h_a(x),f(x))=1$. Suppose the order of nth root of unity ξ is equal to d, it follows from $(g,n)=1$ that $(g,d)=1$. Therefore, the order of $\xi^{kg^{m-i}}$ is equal to to $d/(d,kg^{n-i})=d/(d,k)$, this implies that $\lambda_{1k},\lambda_{2k},\cdots,\lambda_{nk}$ are equal to zero or $\lambda_{1k},\lambda_{2k},\cdots,\lambda_{nk}$ are not equal to zero for fixed k, From (3.10)、(3.6)、(3.7) and (3.2), we know that

$$\mathrm{vank}\,A^m=\mathrm{vank}\,B_m=\mathrm{vank}\,A \tag{3.11}$$

(3.11) implies that the order of any Jordan block of A corresponding to zero eignevalue is equal to one.

Therefore A can be diagonalized.

Corollary 3.2 Any rational g-circulant of ordet n is diagonalization matrix, if n is prime.

4. Fast Inversion of g-Circulant

Let A be invertible g-circulant with the first row $(a_0,a_1,\cdots,a_{n-1})$, it follows from Proposition 2.3 and 2.7, that

$$A=Q_g\sum_{i=0}^{n-1}a_iR^i \quad (g,n)=1$$

Furhtermore. By proposition 2.6 and 2.4, there exist n numbers $c_0,c_1,\cdots,c_{n-1}$. such that

$$A^{-1}=Q_g^{-1}\sum_{i=0}^{n-1}c_iR^i \tag{4.1}$$

and

$$A^{-1}A=Q_g^{-1}Q_g\Big(\sum_{i=0}^{n-1}c_iR^{ig}\Big)\Big(\sum_{i=0}^{n-1}a_iR^i\Big)=\Big(\sum_{i=0}^{n-1}c_iR^{ig}\Big)\Big(\sum_{i=0}^{n-1}a_iR^i\Big)$$

Hence $c=\sum_{i=0}^{n-1}c_iR^{ig}$ is the inversion of the matrix $B=\sum_{i=0}^{n-1}a_iR^i$. By applying Propo sition 1.4, we known that B can be diagonalized by Fourie matrix, i.e.

$$B=F^{-1}\mathrm{diag}(\mu_0,\mu_2,\cdots,\mu_{n-1})F$$

where μ_i $(i=0,1,\cdots,n-1)$ are given by (2.5), and therefore

© 1995-2005 Tsinghua Tongfang Optical Disc Co., Ltd. All rights reserved.

$$B^{-1} = F^{-1}\mathrm{diag}(_0^{-1}, \cdots, \mu_{n-2}^{-1})F \tag{4.2}$$

Algorithm Alg-C (Algorithm for Inverting g-Circualant)

1. Compute $\mu_k = \sum_{i=0}^{n-1} a_i \omega^{ki}$ $(k=0,1,\cdots,n-1)$ by FFT

2. Compute $\mu_0^{-1}, \mu_2^{-1}, \cdots, \mu_{n\ 1}^{-1}$

3. Compute $b_0, b_1, \cdots, b_{n-1}$ Via $\mu_k^{-1} = \sum_{i=0}^{n-1} b_i \omega^{ki}$ by using FFT

4. Compute $a_i \equiv ig(\mathrm{mod}\, n)$

5. Compute non-negative integers l_1 and l_2 such that $l_1 g + l_2 n = 1$ by Eulidean's algorithm

We claim that $A^{-1} = Q^{l_2} \sum_{i=0}^{n-1} ba_i R^i$. This is because $a_i \neq a_j$ if and only if $i \neq j$. Suppose that there exist non-negative integers i, j such that $a_i = a_j$ i.e. $ig \equiv ig$ $(\mathrm{mod}\, n)$ Then, there exist a non-negative inleger q such that $ig - jg = qn$, i.e. $(i-j)g = qn$. Since $(g,n)=1$, then $n \mid (i-j)$ contridicats $|i-j| \leqslant n-1$.

It requires $O(n \log n)$ operations at stages 1 and 3 and $O(n)$ operations at stages 1. and 5. The time complexity is $O(n \log n)$.

References

[1] P.J.Davis, Circulant Matrices, John Wiley & Sons New York, 1979.

[2] You Zhaoyong, Lu Hao, Some properties of g-circulant matrices and solutton of g-ciculant systems (submitted to J. Appl. Math.)

[3] Mingkui Chen, SIAM. J. Numer. Anal, 24(1987), 668—683.

[4] A. V. Aho, J.E.Hopcroft, and J. D. Ullman, The Desigh and Analysis of Computer Algorithms, Addison-Wesley, Reading, Mass, 1974.

[5] C. W. H. Lam, J.Combin Theory Ser. A 23 (1977) 140—147.

[6] D. E. Knuth, J. Combin. Theory Ser. A 8(1970) 376—390.

[7] H. J. Rysor, Linear Algebra and Appl. 3 (1970) 451—460.

[8] K. Wang, J.Combin. Theory Ser. A 33(1982) 287—296.

[9] V. Strassen, Numer. Math. 13(1969) 354—356.

[10] D. Coppersith and S. SIAM, J. Comput 11:3 (1982) 472—497.

有理*g*-轮换阵之性质及*g*-轮换阵求逆的计算复杂性

游兆永　路浩

(西安交通大学数学系)

摘要　本文利用本原多项式在有理数域上的不可约性及 n 次本原根的性质．证明了若 $(g, n)=1$，则 n 阶有理 g-轮换阵为可对角化矩阵．进一步利用快速富里叶变换(FFT)给出了 g-轮换阵之求逆算法．算法的主要运算为FFT的计算，因此时间复杂性为 $O(n\log n)$．其中 (g,n) 表示整数，g, n 的最大公约数．

© 1995-2005 Tsinghua Tongfang Optical Disc Co., Ltd. All rights reserved.