ON QUASI-g-CIRCULANT MATRICES

N. Zagaglia Salvi(*)
Dipartimento di Matematica
Politecnico di Milano
P.za L. da Vinci 32
20133 Milano, Italy

ABSTRACT

A matrix Q of order n is called k-quasi-g-circulant if it satisfies

$$P^k Q = QP^{kg}$$

where P represents the permutation (1 2 ... n), $(n,g)=1$ and the exponents are mod n.
We prove that if $(k,n)=h$, a matrix Q is k-quasi-g-circulant if and only if it is h-quasi-g-circulant; then Q is a block g-circulant matrix of type (q,h) and we give a characterization for these matrices. Moreover we define a perfect k-quasi-g-circulant permutation and we prove that the set of these permutations is an imprimitive group of order $\phi(k)kq^k$, where $\phi(k)$ is the Euler function of k, that is the number of positive integers not greater than and prime to k.

(*) This research was supported by the Ministero della Pubblica Istruzione.

INTRODUCTION

Recall that a matrix C of order n is g-circulant if it is $PC = CP^g$, where P represents the permutation $\pi = (1\ 2\ \dots\ n)$.
We call a matrix Q of order n k-quasi-g-circulant if it satisfies

$$P^k Q = QP^{kg} \tag{1}$$

where $k \in [1,n-1]$ and $(g,n)=1$.
In this paper we prove some properties of these matrices.
In particular we prove that, if $(k,n)=h$, a matrix Q is k-quasi-g-circulant if and only if it is h-quasi-g-circulant; then Q is a block g-circulant matrix of type (q,h) and we give a characterization for these matrices.
Moreover we define a perfect k-quasi-circulant permutation and we prove that the set of these permutations is an imprimitive group of order $\phi(k)kq^k$, where $\phi(k)$ is the Euler function of k, that is the number of positive integers not greater than and prime to k.

1. Let $Q = [q_{ij}]$ be a k-quasi-g-circulant matrix of order n; from (1) it follows also $P^{ik}Q = QP^{ikg}$, $1 \leq i \leq n$.
If $(k,n)=1$, the integers ik, taken modulo n, are distinct. Then, there exists an integer $j \in [1,n-1]$ such that $jk \equiv 1 \pmod{n}$ and $PQ=QP^g$ is satisfied, i.e. Q is g-circulant.

If $(k,n)=h>1$ and $n=hq$, the integers ik are not distinct.
The minimum integer j such that $jk \equiv 0 \pmod{n}$ is q. Then the elements taken modulo n ik , $1 \leq i \leq q$, are repeated h times. Moreover it is easy to see that there exists a $j \in [1,q]$ such that $jk \equiv h \pmod{n}$ and Q satisfies $P^h Q = QP^{hg}$.

Now, if $QP^{hg} = B = [b_{ij}]$ and $P^h Q = C = [c_{ij}]$, from (1) it follows

$$b_{ij} = q_{i\ j-hg}\ ,\quad c_{ij} = q_{i+h\ j}\ ;$$

since $B = C$, we have $q_{i\ j-hg} = q_{i+h\ j}$, where the indices are mod n.
Then we obtain the sequence

$$q_{r\ s} = q_{r+h\ s+hg} = \dots = q_{r+(n-1)h\ s+(n-1)hg} \tag{2}$$

$r,s \in [1,h]$.

Since the minimum positive integer j such that $r+jh \equiv r \pmod n$ is $j=q$, from (2) we obtain that the elements belonging to the rows

$$r,\ r+h,\ \dots,\ r+(q-1)h$$

and to the columns

$$s,\ s+hg,\ \dots,\ s+(q-1)hg$$

are coincident.

So the row $r+th$, $1 \leq r \leq h$ and $1 \leq t \leq q-1$, of Q is obtained from the row $r+(t-1)h$ by shifting cyclically every element of hg positions to the right. Then the h-quasi-g-circulant matrix Q is obtained by taking arbitrarily the h first rows and shifting them cyclically hg positions to the right in order to obtain the next rows.

It is easy to see that if the h first rows are partitioned into q matrices $A_1, A_2, \dots, A_q$, we have

$$Q = \begin{bmatrix} A_1 & A_2 & \dots & A_q \\ A_{q-g+1} & A_{q-g+2} & \dots & A_{q-g} \\ A_{q-2g+1} & A_{q-2g+2} & \dots & A_{q-2g} \\ \dots & & & \\ A_{g+1} & A_{g+2} & \dots & A_g \end{bmatrix} .$$

So Q is a block g-circulant matrix of type (q,h) and we obtain the following

THEOREM 1.1 - A matrix Q of order n satisfies $P^k Q = QP^{kg}$, where $(n,k)=h \geq 1$ and $n=hq$, if and only if it satisfies $P^h Q = QP^{hg}$. Then Q is a block g-circulant matrix of type (q,h).

THEOREM 1.2 - A matrix Q of order n=hq is block g-circulant of type (q,h) if and only if it satisfies

$$(P_q \otimes I_h) Q = Q ((P_q)^g \otimes I_h). \tag{3}$$

Proof. The matrices $P_q \otimes I_h$ and $(P_q)^g \otimes I_h$ are block g-circulant of type (q,h) and are given by

$$P_q \otimes I_h = \begin{bmatrix} O_h & I_h & O_h & \cdots & O_h \\ O_h & O_h & I_h & \cdots & O_h \\ \cdots & & & & \\ I_h & O_h & O_h & \cdots & O_h \end{bmatrix}$$

and

$$(P_q)^g \otimes I_h = \begin{bmatrix} O_h & O_h & \cdots & I_h & & \cdots & O_h \\ O_h & O_h & \cdots & O_h & I_h & \cdots & O_h \\ & & & & & & \\ \cdots & & & & & & \\ O_h & \cdots & I_h & O_h & & \cdots & O_h \end{bmatrix}$$

where g is the number of O_h before I_h on the first row.
Then these permutation matrices coincide respectively with P^h and P^{hg}.
From Theorem 1.1 it follows that , if Q satisfies (3), then it is block g-circulant of type (q,h).
Conversely, since the formal rules of block multiplication are the same as for ordinary multiplication, if Q is block g-circulant, the argument followed in [2] to prove that a g-circulant matrix satisfies $PQ=QP^g$, is valid when interpretated blockwise.

THEOREM 1.3 - A matrix A of order n satisfies $P^hA=AP^{hg}$, where $(n,g)=1$, if and only if it satisfies $AP^h=P^{hi}A$, where $i \equiv g^{\phi(n)-1} \pmod{n}$.

Proof. If A satisfies $P^hA=AP^{hg}$, then we have $P^{jh}A=AP^{jhg}$, $1 \leq j \leq n$.
If i is the minimum positive integer such that $ig \equiv 1 \pmod{n}$, then

we obtain $AP^h=P^{hi}A$. By a Euler's theorem we have $g^{\phi(n)} \equiv 1 \pmod n$; then $g\,g^{\phi(n)-1} \equiv 1$ and, since for $(n,g)=1$ the solution to $gx \equiv 1 \pmod n$ is unique mod n, $i \equiv g^{\phi(n)-1} \pmod n$.
Conversely, if it is $AP^h=P^{hi}A$, where $(n,i)=1$, by the same considerations we obtain $P^hA=AP^{hg}$, where $g \equiv i^{\phi(n)-1} \pmod n$.

Many properties of the g-circulant matrices can be exspressed in terms of block g-circulant matrices.
Among these, we consider the following

THEOREM 1.4- If A is a block g-circulant and B is a block h-circulant, then AB is a block gh-circulant.

The proof follows as for g-circulant matrices.

COROLLARY 1.5 - The product of two block g-circulant matrices is also block g-circulant only for $g \equiv 1 \pmod n$.

Proof. By Theorem 1.4 the product of two block g-circulant matrices is block g^2-circulant; then $g^2 \equiv g \pmod n$ only for $g \equiv 1 \pmod n$.

2. If we consider block g-circulant permutation matrices, from Corollary 1.5 it follows that only for g=1 the corresponding permutations form a group.
Recall that a 1-circulant is a circulant.

PROPOSITION 2.1- The number of h-quasi-g-circulant permutation matrices of order n=hq is $h!q^h$.

Proof. By Theorem 1.1 only the first h rows of a h-quasi-g-circulant matrix Q are arbitrary.

For the position of the element 1 on the first row there are n possibilities. Since other q-1 columns of Q have the element 1 fixed, for the position of the element 1 on the second row there are n-q possibilities.
In a similar way, for the element 1 on the i-th row, $1 \leq i \leq h$, there are $n-(i-1)q$ possibilities and the number of k-quasi-circulant permutations Q of order $n=hq$ and $(k,n)=h \geq 1$, is $n(n-q)\ldots(n-(h-1)q)=h!q^h$.

PROPOSITION 2.2 - The set of permutations corresponding to h-quasi-circulant matrices of order $n=hq$ forms an imprimitive permutation group Γ of order $h!q^h$ and rank $q+1$.

Proof. The set Γ of permutations corresponding to h-quasi-circulant matrices is the centralizer of π^h on the symmetric group S_n. As P is h-quasi-circulant, then Γ is a transitive group.
Moreover the disjoint sets $H_i = \{i, i+h, \ldots, i+(q-1)h\}$, $1 \leq i \leq h$, are nontrivial blocks for Γ and Γ is imprimitive.
In fact, let $g \in \Gamma$ and $g(i)=j$ where $1 \leq j \leq n$; then we have $g(i+rh)=j+rh$, $0 \leq r \leq q-1$. Consequently $gH_i = \{j, j+h, \ldots, j+(q-1)h\}$ is one of the sets H_i and either $gH_i = H_i$ or $gH_i \cap H_i = \emptyset$.
The order of Γ follows from Prop. 2.1.
Finally, let Γ_x the stabilizer of x, for $x \in [1,n]$. If $g \in \Gamma_x$, we have $g(x)=x$; then it follows that $g(x+rh)=x+rh$, where $0 \leq r \leq q-1$ and the integers are modulo n.
Since Γ_x is transitive on $N - \{x+rh \mid 0 \leq r \leq q-1\}$, we get that the orbits of Γ_x are $q+1$, q of length 1 and 1 of length $n-q=(h-1)q$.

As in a h-quasi-circulant permutation matrix Q of order $n=hq$ only the h first rows are arbitrary, it follows that the permutation α corresponding to Q is determined by the elements $a_i \in [1,n]$ such that $\alpha(i)=a_i$ for $1 \leq i \leq h$ and $a_i \not\equiv a_j \pmod h$, $i \neq j$. Note that $\alpha(i+rh)=a_{i+rh}=a_i+rh$, $r \in [1,q-1]$.
Remark that, if α is a circulant or g-circulant permutation, there exists an integer j prime to n such that $\alpha(i+1) - \alpha(i) \equiv j \pmod n$.

Now we give a generalization of these permutations.

DEFINITION 2.3 - We call a permutation α , corresponding to a h-quasi-circulant matrix of order n=hq, <u>j-perfect</u> if there exists an integer $j \in [1,h-1]$ such that

$$a_{i+1} - a_i \equiv j \pmod h \qquad (4)$$

for $i \in [1,h]$.

Since $\alpha(i+rh) = a_i + rh$, we can extend (4) to $i \in [1,n]$.
Moreover from (4) we obtain $a_{i+k} - a_i \equiv kj \pmod h$, $1 \leq k \leq h-1$. Then it is $a_i \equiv a_1+(i-1)j \pmod h$ for $2 \leq i \leq h$; so a perfect h-quasi-circulant permutation α depends on only two integers a_1 and j, apart from the congruence of $\alpha(i)$ modulo h.

PROPOSITION 2.4 - If a h-quasi-circulant permutation is j-perfect, then $(j,h)=1$.

Proof. In fact, if it is $(j,h)=s > 1$ and $h = sh'$, then $a_{h'+1} \equiv a_1+h'j \equiv a_1 \pmod h$, where $h'+1 \leq h$. So the integers $a_1, a_2, \ldots, a_h$ are not distinct mod h.

Denote by Ξ $[\Xi_j]$ the set of $[j]$ -perfect h-quasi-circulant permutations of degree n=hq.

PROPOSITION 2.5 - The order of Ξ_j is hq^h.

Proof. Notice that, if α is a j-perfect h-quasi-circulant permutation dependent on a_1 and j, a_1 can be any element of the set $[1,n]$.
If a_1 is determined, then we can obtain the integers a_i, $2 \leq i \leq h$, by the relation $a_i \equiv a_1+(i-1)j \pmod h$.
As there are q elements that satisfy this relation, we have that, if a_1 is is determined, there are q^{h-1} possibilities; then we obtain hq^h perfect permutations.

If $\phi(h)$ is the Euler function of h, that is the number of positive integers not greater than and prime to h, we have the following

THEOREM 2.6 - The set Ξ is an imprimitive subgroup of Γ of order $\phi(h)hq^h$.

Proof. Prove that the product of two permutations $\alpha,\beta\in\Xi$ is also a member of Ξ. If a_1, j and b_1, k are the integers corresponding to α and β, with j and k prime to h, we have $\beta(\alpha(i)) \equiv \beta(a_1+(i-1)j) \equiv b_1+(a_1+(i-1)j-1)k \pmod h$. So the difference between the elements corresponding to i+1 and i is jk (mod h). As such a difference does not depend on i and it is prime to h, we have that $\alpha\beta$ is perfect.
Moreover, if $\alpha\in\Xi$, then also $\alpha^{-1}\in\Xi$.
If $\alpha(s)=a_i$ and $\alpha(p)=a_i+1$, where $s,p\in[1,n]$, $a_i \equiv a_1+(s-1)j \pmod h$ and $a_i+1 \equiv a_1+(p-1)j \pmod h$, we have $\alpha^{-1}(a_i)=s$ and $\alpha^{-1}(a_i+1)=p$.
By calculating $(a_i+1)-a_i$, we get that p-s satisfies the relation $(p-s)j \equiv 1 \pmod h$; then p-s does not depend on a_i and it is prime to h.
So α^{-1} is perfect.
Being π 1-perfect, Ξ is a transitive group and has the same nontrivial blocks as Γ.
From Prop. 2.4 and Prop. 2.5 we obtain that the order of Ξ is $\phi(h)hq^h$.

COROLLARY 2.7 - If a subgroup of Γ contains a j-perfect permutation, then it contains t-perfect permutations, for t coincident with $j, j^2, \ldots, j^{q-1}$, where q is the minimum integer such that $j^q \equiv j \pmod h$. Then $q-1 \mid \phi(h)$ and q=h if and only if h is prime.

Proof. In fact, if α is a j-perfect permutation, then, by Theorem 2.6, α^r is j^r-perfect, where $1 \le r \le q-1$ and q is the minimum integer such that $j^q \equiv j \pmod h$. Since by Prop. 2.4 $(j,h)=1$, from the Theorems of Euler and Fermat we obtain that $q-1 \mid \phi(h)$ and q=h if and only if h is prime.

COROLLARY 2.8 - The set of j-perfect h-quasi-circulant permutations is a subgroup of Ξ if and only if $j \equiv 1 \pmod h$.

Proof. By Theorem 2.6, the product of two j-perfect permutations is j-perfect iff $j^2 \equiv j \pmod{h}$; then we have $j \equiv 1 \pmod{h}$. Moreover, if α is j-perfect, then α^{-1} is ρ-perfect, where $\rho j \equiv 1 \pmod{h}$. So, if α is 1-perfect, also α^{-1} is 1-perfect.

If Ψ is the group of 1-perfect h-quasi-circulant permutations of degree $n=hq$, then C_n is a subgroup of Ψ.

We can see a retrocirculant matrix of order 2m can be partitioned into matrices A and B of order m in the following way $\begin{bmatrix} A & B \\ B & A \end{bmatrix}$; hence it is a m-quasi-circulant matrix.

REMARK 2.9 - The dihedral group D_{4m} is a subgroup of the perfect m-quasi-circulant permutation group Ξ of degree 2m.

Proof. In fact, the generators of D_{4m} are the circulant permutation $\pi = (1\ 2\ \ldots\ 2m)$ and the retrocirculant permutation $\sigma = (1\ 2m)(2\ 2m-1)\ldots(m\ m+1)$; hence every element of D_{4m} is m-quasi-circulant. Moreover, since π is a 1-perfect permutation and σ is a (m-1)-perfect permutation, every element of D_{4m} is t-perfect for t coincident with 1, m-1, $(m-1)^2 \equiv 1 \pmod{m}$. So D_{4m} is a subgroup of Ξ.

The group D_8 acting on the corners of a square is the 2-quasi-circulant permutation group of degree 4.

REFERENCES

[1] N.L. Biggs and A.T. White, *Permutation Groups and Combinatorial Structures* , Cambridge University Press, 1979.

[2] P.J. Davis, *Circulant matrices*, A Wiley-Interscience Publication, 1979.

[3] I.M. Vinogradov, *An introduction to the theory of numbers*, Pergamon Press, London, 1955.

[4] K. Wang, On the generalizations of circulants, *Linear Algebra and Appl.* 25 (1979), 197-218.

[5] K. Wang, On the generalization of a retrocirculant, *Linear Algebra and Appl.* 37(1981), 35-43.