Journal of Mathematics Research; Vol. 6, No. 2; 2014
ISSN 1916-9795 E-ISSN 1916-9809
Published by Canadian Center of Science and Education

The Cyclic Groups and the Semigroups via MacWilliams and Chebyshev Matrices

Ömür Deveci[1] & Yeşim Aküzüm[1]

[1] Department of Mathematics, Faculty of Science and Letters, Kafkas University, Kars, Turkey

Correspondence: Ömür Deveci, Department of Mathematics, Faculty of Science and Letters, Kafkas University, Kars 36100, Turkey. E-mail: odeveci36@hotmail.com

Received: November 13, 2013 Accepted: January 2, 2014 Online Published: April 18, 2014

doi:10.5539/jmr.v6n2p55 URL: http://dx.doi.org/10.5539/jmr.v6n2p55

Abstract

In this paper, we consider the multiplicative orders of the MacWilliams matrix of order $N (M_N)_{ij}$ and the Chebyshev matrix of order $N (D_N)_{ij}$ according to modulo m for $N \geq 1$. Consequently, we obtained the rules for the orders of the cyclic groups and semigroups generated by reducing the MacWilliams and Chebyshev matrices modulo m and the deteminats of these matrices.

Keywords: MacWillams matrix, Chebyshev matrix, group, order

2000 Mathematics Subject Classification: 15A15, 20H25, 15A15, 20F05

1. Introduction

The *rth* Krawtchouk polynomial of order N, is defined as (See Hirvencalo, 2003; MacWilliams & Sloane, 1977)

$$K_r^N(x) = \sum_{i=0}^{r} (-1)^i \binom{N-x}{r-i} \binom{x}{i}$$

where $K_0^0(0) = 1$.

The MacWilliams matrix of order N has been given as (See Gogin & Hirvencalo, 2012; Gogin & Myllari, 2007)

$$(M_N)_{ij} = K_i^N(j) \quad \text{for} \quad 0 \leq i, j \leq N.$$

where $(M_0)\, ij = (1)$.

The *rth* discrete Chebyshev polynomial of order N, is defined as (See Bateman & Erdelyi, 1953; Hirvencalo, 2003)

$$D_r^N(x) = \sum_{i=0}^{r} (-1)^i \binom{r}{i} \binom{N-x}{r-i} \binom{x}{i}$$

where $D_0^0(0) = 1$.

In Gogin and Hirvencalo (2012), the Chebyshev matrix of order N has been given as

$$(D_N)_{ij} = D_i^N(j) \quad \text{for} \quad 0 \leq i, j \leq N.$$

Note that if $N = 0$, $(D_0)\, ij = (1)$. It is important to note that $(M_1)\, ij = (D_1)\, ij = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

Recently, MacWilliams and Chebyshev matrices and their properties have been studied by some authors; see for example (Bateman & Erdelyi, 1953; Gluesing-Luerssen & Schneider, 2008; Gogin & Hirvencalo, 2012, 2007; Gogin & Myllari, 2007; Hirvencalo, 2003; MacWilliams & Sloane, 1977; Pan & Wang, 2012; Szegö, 1975). Lü and Wang (2007) obtained the rules for the orders of the cyclic groups generated by reducing the k-generalized Fibonacci matrix modulo m. Deveci and Karaduman (2012a) extended the concept to Pascal and generalized Pascal matrices. Now we extend the concept to the MacWilliams matrix of order $N (M_N)_{ij}$ and the Chebyshev matrix of order $N (D_N)_{ij}$ for $N \geq 1$.

In this paper, the usual notation p is used for a prime number.

2. Method

For given a matrix $M = \left[m_{ij}\right]$ with m_{ij}'s being integers, $M\,(\text{mod}\ m)$ means that each element of M are reduced modulo m, that is, $M\,(mod\ m) = \left(m_{ij}\,(mod\ m)\right)$. Let us consider the set $\langle M\rangle_m = \left\{M^i\,(\text{mod}\ m)\middle|\, i \geq 0\right\}$. If $\gcd(m, \det M) = 1$, then the set $\langle M\rangle_m$ is a cyclic group; if $\gcd(m, \det M) \neq 1$, then the set $\langle M\rangle_m$ is a semigroup. Let the notation $|\langle M\rangle_m|$ denotes the order of $\langle M\rangle_m$.

By matrix algebra it is easy to prove that

$$\left((M_N)_{ij}\right)^{2k} = \left[m_{ij}\right]_{(N+1)\times(N+1)} = \begin{bmatrix} 2^{kN} & 0 & \cdots & 0 & 0 \\ 0 & 2^{kN} & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 2^{kN} \end{bmatrix}, \quad (k \geq 0) \tag{1}$$

that is, the matrix $\left((M_N)_{ij}\right)^{2k}$ is an $(N+1)\times(N+1)$ diagonal matrix with $2^{kN}, \cdots, 2^{kN}$ as diagonal entries.

Also, we obtain $\det\left((M_N)_{ij}\right)$, $(N \geq 1)$ as following

$$\det\left((M_N)_{ij}\right) = \begin{cases} -2^{\frac{N^2+N}{2}}, & N \equiv 1, 2 \bmod 4, \\ 2^{\frac{N^2+N}{2}}, & N \equiv 0, 3 \bmod 4. \end{cases} \tag{2}$$

It is easy to see from (2) that $\langle M_N\rangle_m$ is a cyclic group if m is an odd integer and $\langle M_N\rangle_m$ is a semigroup if m is an even integer.

3. Results

Theorem 3.1 *If m is an odd integer, the order of the cyclic group $\langle M_N\rangle_m$ is $2k$ where k is least positive integer such that $2^{kN} \equiv 1 \pmod m$.*

Proof. It is easy to see from (1) that $\left((M_N)_{ij}\right)^{2k}\,(\text{mod}\ m) \equiv I_{(N+1)}$ where $I_{(N+1)}$ is identity matrix of size $(N+1)\times(N+1)$. If we choose k as least positive integer such that $2^{kN} \equiv 1 \pmod m$, then we obtain $|\langle M_N\rangle_m| = 2k$. □

Theorem 3.2 *Let m be an even integer, then two cases occur for order of the semigroup $\langle M_N\rangle_m$:*

(i) If $m = 2^u$ $(u \in \mathbb{N})$, then the order of the semigroup $\langle M_N\rangle_{2^u}$ is $2k$ where k is least positive integer such that $2^{kN} \equiv 0 \pmod m$.

(ii) If $m = 2^u t$ $(u \in \mathbb{N})$ such that t is an odd integer, then $|\langle M_N\rangle_{2^u t}| = |\langle M_N\rangle_{2^u}| + |\langle M_N\rangle_t| - 1$.

Proof. (i) It is easy to see from (1) that

$$\left((M_N)_{ij}\right)^{2k}\,(\text{mod}\ m) \equiv 0_{(N+1)}$$

where $0_{(N+1)}$ is zero matrix of size $(N+1)\times(N+1)$. If we choose k as least positive integer such that $2^{kN} \equiv 0 \pmod m$, then we obtain $|\langle M_N\rangle_m| = 2k$.

(ii) Let $|\langle M_N\rangle_t| = 2\alpha$ and $|\langle M_N\rangle_{2^u}| = 2\beta$. Then

$$2^{\alpha N} = k_1 t + 1 \quad \text{and} \quad 2^{\beta N} = k_2 2^u$$

where $k_1, k_2 \in \mathbb{N}$ and $\gcd(t, k_2) = 1$. Thus, we have $2^{(\alpha+\beta)N} \equiv 2^u k_2\,(\text{mod}\ m)$, that is $\left((M_N)_{ij}\right)^{2\alpha+2\beta}\,(\text{mod}\ m) \equiv \left((M_N)_{ij}\right)^{2\beta}$. So, we get $|\langle M_N\rangle_{2^u t}| = |\langle M_N\rangle_{2^u}| + |\langle M_N\rangle_t| - 1$. □

Remark 3.1 If p is the greatest prime factor $\det\left((D_N)_{ij}\right)$, then $p!|\det\left((D_N)_{ij}\right)$.

Theorem 3.3 *Let $\gcd\left(p,\ \det\left((D_N)_{ij}\right)\right) = 1$ and let t be the largest positive integer such that $\left|\langle D_N\rangle_p\right| = \left|\langle D_N\rangle_{p^t}\right|$. Then $\left|\langle D_N\rangle_{p^\alpha}\right| = p^{\alpha-t}\left|\langle D_N\rangle_p\right|$ for every $\alpha \geq t$. In particular, if $\left|\langle D_N\rangle_p\right| \neq \left|\langle D_N\rangle_{p^2}\right|$, then $\left|\langle D_N\rangle_{p^\alpha}\right| = p^{\alpha-1}\left|\langle D_N\rangle_p\right|$ holds for every $\alpha > 1$.*

Proof. We first note that $\langle D_N \rangle_{p^u}$ is a cyclic group for every $u \geq 1$. Let θ be a positive integer and let $|\langle D_N \rangle_m|$ be denoted by $h_N(m)$. Since $(D_N)_{ij}^{h_N(p^{\theta+1})} \equiv I_{N+1} \pmod{p^{\theta+1}}$, that is, $(D_N)_{ij}^{h_N(p^{\theta+1})} \equiv I_{N+1} \pmod{p^{\theta}}$, we get that $h_N(p^\theta)$ divides $h_N(p^{\theta+1})$. On the other hand, writing $(D_N)_{ij}^{h_N(p^\theta)} = I_{N+1} + \left(a_{ij}^{(\theta)} p^\theta\right)$, we have

$$(D_N)_{ij}^{h_N(p^\theta)p} = \left(I_{N+1} + \left(a_{ij}^{(\theta)} p^\theta\right)\right)^p = \sum_{i=0}^{p} \binom{p}{i} \left(a_{ij}^{(\theta)} p^\theta\right)^i \equiv I_{N+1} \pmod{p^{\theta+1}}.$$

So we get that $h_N(p^{\theta+1}) \,\big|\, h_N(p^\theta)\, p$. Thus, $h_N(p^{\theta+1}) = h_N(p^\theta)$ or $h_N(p^{\theta+1}) = h_N(p^\theta)\, p$, and the latter holds if, and only if, there is a $a_{ij}^{(\theta)}$ such that $p \nmid a_{ij}^{(\theta)}$. Since $h_N(p^t) \neq h_N(p^{t+1})$, there is an $a_{ij}^{(t+1)}$ such that $p \nmid a_{ij}^{(t+1)}$, therefore, $h_N(p^{t+1}) \neq h_N(p^{t+2})$. The proof is finished by induction on t. □

Theorem 3.4 *Let* $\gcd\left(m, \det\left((D_N)_{ij}\right)\right) = 1$ *and let* $m = \prod_{i=1}^{t} p_i^{e_i}$, $(t \geq 1)$ *where* p_i*'s are distinct primes, then* $|\langle D_N \rangle_m| = \mathrm{lcm}\left[\left|\langle D_N \rangle_{p_1^{e_1}}\right|, \left|\langle D_N \rangle_{p_2^{e_2}}\right|, \cdots, \left|\langle D_N \rangle_{p_t^{e_t}}\right|\right]$.

Proof. Let $\left|\langle D_N \rangle_{p_k^{e_k}}\right| = \lambda_k$ for $1 \leq k \leq t$ and let $|\langle D_N \rangle_m| = \lambda$. Then we have the entry (i, j) of

$$(D_N)_{ij}^{\lambda_k} = \begin{cases} p_k^{e_k} \varepsilon_{ij} K_i^N(j), & i > j, \\ p_k^{e_k} \varepsilon_{ij} K_i^N(j) + 1, & i = j, \\ p_k^{e_k} \varepsilon_{ij} K_i^N(j), & i < j, \end{cases}$$

and the entry (i, j) of

$$(D_N)_{ij}^{\lambda} = \begin{cases} m\varepsilon'_{ij} K_i^N(j), & i > j, \\ m\varepsilon'_{ij} K_i^N(j) + 1, & i = j, \\ m\varepsilon'_{ij} K_i^N(j), & i < j, \end{cases}$$

where ε_{ij} and ε'_{ij} are integers for $0 \leq i, j \leq N$.

Therefore $(D_N)_{ij}^{\lambda}$ is of the form $c \cdot (D_N)_{ij}^{\lambda}$, $(c \in \mathbb{N})$ for all values of k, and since any such number gives λ, we conclude that $\lambda = \mathrm{lcm}[\lambda_1, \lambda_2, \cdots, \lambda_t]$. □

Corollary 3.1 *The orders of the semigroups* $\langle D_2 \rangle_{2^k}$ *and* $\langle D_2 \rangle_{3^k}$ *are* $2k + 1$ *and* $2^k(k-1) + 2k + 1$*, respectively.*

Proof. We first note that $\langle D_2 \rangle_{2^k}$ and $\langle D_2 \rangle_{3^k}$ are semigroups for every $k \geq 1$ since $\det\left((D_2)_{ij}\right) = -12$. By matrix algebra it is easy to prove that

$$(D_2)_{ij}^{2k} = \begin{bmatrix} 2^{2k} & 2^{k-1}\left(2^k - 3^k\right) & 0 \\ 0 & 6^k & 0 \\ 2^k\left(2^k - 3^k\right) & 2^{k-1}\left(2^k - 3^k\right) & 6^k \end{bmatrix}$$

and

$$(D_2)_{ij}^{2k+1} = \begin{bmatrix} 2^k\left(2^{k+1} - 3^k\right) & 2^{2k} & 6^k \\ 2 \cdot 6^k & 0 & -2 \cdot 6^k \\ 2^k\left(2^{k+1} - 3^k\right) & 2^k\left(2^k - 3^{k+1}\right) & 6^k \end{bmatrix}$$

for $k \geq 1$. Since $(D_2)_{ij}^{2k+1} \equiv 0_3 \left(mod\ 2^k\right)$ and $(D_2)_{ij}^{2^k(k-1)+2k+2} \equiv (D_2)_{ij}^{2k} \left(mod\ 3^k\right)$, we get that $|\langle D_2 \rangle_{2^k}| = 2k + 1$ and $|\langle D_2 \rangle_{3^k}| = 2^k(k-1) + 2k + 1$. □

4. Discussion

Wall (1960) proved that the lengths of the periods of the recurring sequences obtained by reducing a Fibonacci sequences by a modulo m are equal to the lengths of the of ordinary 2-step Fibonacci recurrences in cyclic groups. The theory is expanded to 3-step Fibonacci sequence by Ozkan, Aydin, and Dikici (2003). Lü and Wang (2007) contributed to the study of the Wall number for the k-step Fibonacci sequence. In (Deveci, 2011; Deveci & Karaduman, 2012b, to appear; Deveci, to appear), the concept has been extended to some special linear recurrence sequences. In this paper, we obtained the cyclic groups and semigroups generated by reducing the MacWilliams and Chebyshev matrices modulo m. Are there groups such that the lengths of the periods of some special recurrence sequences of elements of these groups are obtained by the orders of these cyclic groups and semigroups?

Acknowledgments

The authors thank the referees for their valuable suggestions which improved the presentation of the paper. This Project was supported by the Commission for the Scientific Research Projects of Kafkas University. The Project number is 2013-FEF-72.

References

Bateman, H., & Erdelyi, A. (1953). *Higher transcendental functions* (Vol. 2). McGraw-Hill.

Deveci, O. (2011). The polytopic-k-step Fibonacci sequences in finite groups. *Discrete Dyn. Nat. Soc., 2011*, Article ID 431840. http://dx.doi.org/10.1155/2011/431840

Deveci, O. (to appear). The Pell-Padovan sequences and the Jacobsthal-Padovan sequences in finite groups. *Util. Math*.

Deveci, O., & Karaduman, E. (2012a). The cyclic groups via the Pascal matrices and the generalized Pascal matrices. *Linear Algebra and Its Applications, 437*, 2538-2545.

Deveci, O., & Karaduman, E. (2012b). The generalized order-k Lucas sequences in Finite groups. *J. Appl. Math., 2012*, Article ID 464580. http://dx.doi.org/10.1155/2012/464580

Deveci, O., & Karaduman, E. (to appear). The Pell sequences in finite groups. *Util. Math*.

Gluesing-Luerssen, H., & Schneider, G. (2008). On the MacWilliams identity for convolutional codes. *IEEE Transations on Information Theory, 54*(4).

Gogin, N., & Hirvencalo, M. (2007). On the generating function of discrete Cheyshev polynomial. *TUCS technical Reports, 819, Turku Centre for Computer Science*.

Gogin, N., & Hirvencalo, M. (2012). Recurrent construction of MacWilliams and Chebyshev matrices. *Fundamenta Informaticae, 116*(1-4), 93-110.

Gogin, N., & Myllari, A. A. (2007). The Fibonacci-Padovan sequence and MacWilliams transform matrices. *Programing and Computer Software, Published in Programmirovanie, 33*(2), 74-79.

Hirvencalo, M. (2003). Studies on Boolean functions related to quantum computing (Ph.D. Thesis, Univesity of Turku).

Lü, K., & Wang, J. (2007). k-step Fibonacci sequence modulo m. *Util. Math., 71*, 169-178.

MacWilliams, F. J., & Sloane, N. J. A. (1977). *The theory of error-correcting codes*. North-Holland.

Ozkan, E., Aydin, H., & Dikici, R. (2003). 3-step Fibonacci series modulo m. *Applied Mathematics and Computation, 143*, 165-172.

Pan, J. H., & Wang, R. (2012). Uniform asymptotic expansions for the discrete Chebyshev polynomials. *Studies in Applied Mathematics, 128*(4), 337-384.

Szegö, G. (1975). *Orthogonal polynomials* (Vol. 23). Providence, Rhode Island, American Mathematical Society, Colloquium Publications.

Wall, D. D. (1960). Fibonacci series modulo m. *Amer. Math. Monthly, 67*, 525-532.