Gulf Journal of Mathematics
Vol 15, Issue 2 (2023) 160-165

ISSN: 2309-4966
https://doi.org/10.56947/gjom.v15i2.1412

VECTOR-CIRCULANT MATRICES AND CODES OVER RINGS

HORACIO TAPIA-RECILLAS[1] AND JUAN ARMANDO VELAZCO-VELAZCO[2*]

Abstract. Circulant matrices are of interest on their own as well as for their relevance to several areas of mathematics. In this note vector-circulant matrices over commutative rings are introduced and related results are given. Vector-circulant based additive codes are presented over a particular finite ring.

1. Introduction and preliminaries

Circulant matrices are interesting by themselves and can be found in several areas of mathematics including their relation with the Fourier transform and coding theory, particularly with quasi-cyclic, double circulant and based additive codes. Various generalizations of circulant matrices such as negacirculant, twistulant matrices have been applied in a number of directions, specially in coding theory, for example circulant based and double circulant codes with optimal and extremal parameters.

In this note, following [5], vector-circulant matrices over a commutative ring are introduced and results on the structure of these matrices are given (Section 2). As an application, vector-circulant based additive codes over finite rings are introduced in Section 3 and illustrated with codes over the ring $R_2 = \mathbb{F}_2 + u\mathbb{F}_2$ with $u^2 = 0$.

2. Some results

Let n be a positive integer, R a commutative ring and $\mathcal{U}(R)$ the group of units of R. Let $\mathcal{M}_n(R)$ be the ring of $n \times n$ matrices over the ring R. Let $\lambda = (\lambda_0, \lambda_1, \ldots, \lambda_{n-1}) \in R^n$ and consider the matrix,

$$M_\lambda = \begin{bmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \ldots & \vdots & \ldots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ \lambda_0 & \lambda_1 & \lambda_2 & \ldots & \lambda_{n-1} \end{bmatrix}.$$

Date: Received: Aug 31, 2023; Accepted: Dec 3, 2023.
* Corresponding author.
2010 *Mathematics Subject Classification.* 13M99, 15B33, 94B99.
Key words and phrases. circulant matrices, finite rings, additive codes.

Let $\rho_\lambda : R^n \longrightarrow R^n$ be the linear mapping determined by the matrix M_λ: $\rho_\lambda(\mathbf{a}) = \mathbf{a}M_\lambda$ where $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1}) \in R^n$.

For an element $\mathbf{a} \in R^n$ let

$$\operatorname{circ}_\lambda(\mathbf{a}) = \begin{bmatrix} \mathbf{a} & \rho_\lambda(\mathbf{a}) & \ldots & \rho_\lambda^{n-1}(\mathbf{a}) \end{bmatrix}^t,$$

where $\rho_\lambda^i(\mathbf{a}) = \mathbf{a}M_\lambda^i$, $i = 1, \ldots, n-1$ and $[*]^t$ denotes the transpose matrix. This is called the λ-vector-circulant matrix. For $\lambda = (1, 0, \ldots, 0)$ this is the classic circulant matrix; for $\lambda = (-1, 0, \ldots, 0)$ the matrix is the negacirculant matrix ([3]) and, more generally, for $\lambda = (\alpha, 0, \ldots, 0)$ the matrix is the α-twistulant matrix, where α is an element of the ring R.

Example 2.1. Consider the ring $\mathbb{F}_2 + u\mathbb{F}_2 = \{0, 1, u, 1+u \mid 0, 1 \in \mathbb{F}_2, u^2 = 0\}$ and let $\lambda = (1, 0, u) \in R^3$. Then,

$$M_\lambda = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & u \end{bmatrix}$$

and

$$\operatorname{circ}_\lambda(1, u, 0) = \begin{bmatrix} 1 & u & 0 \\ 0 & 1 & u \\ u & 0 & 1 \end{bmatrix}.$$

Let $e_1, e_2, \ldots, e_n$ be the canonical elements of R^n and let $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1}) \in R^n$. An easy calculation shows that

$$\operatorname{circ}_\lambda(\mathbf{a}) = \sum_{i=0}^{n-1} a_i \operatorname{circ}_\lambda(e_{i+1}).$$

This relation states that the R-module of the λ-vector-circulant matrices, $\operatorname{Circ}_{n,\lambda}(R)$, is generated over R by the set $\{\operatorname{circ}_\lambda(e_i), i = 1, 2, \ldots, n\}$. Furthermore, we have the following,

Proposition 2.2. *The elements of the set* $\{\operatorname{circ}_\lambda(e_i),\ i = 1, 2, \ldots, n\}$ *are* R*-linearly independent.*

Proof. Let $\sum_{i=1}^n \alpha_i \operatorname{circ}_\lambda(e_i) = 0$ for elements $\alpha_1, \alpha_2, \ldots, \alpha_n$ in the ring R. A direct calculation shows that the first row of the matrix $\sum_{i=1}^n \alpha_i \operatorname{circ}_\lambda(e_i)$ is $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ which by assumption is equal to zero, showing that $\alpha_1 = \alpha_2 = \ldots = \alpha_n = 0$. □

An interesting property of the matrix M_λ is the following,

Proposition 2.3. *The matrix* M_λ *is row equivalent to the diagonal matrix* $D = \operatorname{diag}(\lambda_0, 1, 1, \ldots, 1)$.

Proof. Let A_i denote the i-th row of the matrix M_λ. Interchanging the rows $A_i \leftrightarrow A_{i-1}$ $i = n, n-1, \ldots, 2$ successively on M_λ, we have the matrix

$$\begin{bmatrix} \lambda_0 & \lambda_1 & \lambda_2 & \ldots & \lambda_{n-1} \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \ldots & \vdots & \ldots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{bmatrix}.$$

Performing the row operations $A_1 \longrightarrow A_1 - \lambda_{i-1}A_i$ with $i = 2, 3, \ldots, n$ on this new matrix results in the diagonal matrix $D = \mathrm{diag}(\lambda_0, 1, 1, \ldots, 1)$. □

A consequence of this result is,

Corollary 2.4. *The matrix M_λ is invertible if and only if λ_0 is a unit of the ring R. Hence the introduced linear mapping ρ_λ determined by the matrix M_λ is bijective if and only if λ_0 is a unit of the ring R.*

Example 2.5. Let

$$R = \mathbb{Z}_4 + u\mathbb{Z}_4 = \{a + bu \mid a, b \in \mathbb{Z}_4,\ u^2 = 0\},$$

with the natural operations of sum and product. This is a finite local commutative ring with identity and maximal ideal $\mathfrak{m} = \langle 2, u\rangle$. Let $\lambda = (3 + u, 1, 0, 2, u)$, $M_\lambda \in \mathcal{M}_5(R)$ given by

$$M_\lambda = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 3+u & 1 & 0 & 2 & u \end{bmatrix}.$$

Then, performing $A_5 \leftrightarrow A_4$ followed by $A_i \leftrightarrow A_{i-1}$, $i = 4, 3, 2$ respectively on each new matrix obtained and we have

$$\begin{bmatrix} 3+u & 1 & 0 & 2 & u \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

The operations $A_1 \longrightarrow A_1 - A_2$, $A_1 \longrightarrow A_1 - 2A_4$ and $A_1 \longrightarrow A_1 - uA_5$ give

$$D = \mathrm{diag}(3 + u, 1, 1, 1, 1).$$

Notice that $\det(D) = 3 + u \in \mathcal{U}(R)$ as $(3 + u)^{-1} = 3 + 3u$, therefore M_λ is invertible.

There is also a nice relation between powers of the mapping ρ_λ and powers of the matrix M_λ.

Proposition 2.6. *With the notation as above,*

(1) $M_\lambda^k = \mathrm{circ}_\lambda(\rho_\lambda^k(e_1))$ *for all integers $k \geq 0$.*

(2) $M_\lambda^i = \mathrm{circ}_\lambda(e_{i+1})$ *for* $0 \le i \le n-1$, *where* $M_\lambda^0 = I_n$, *the identity matrix of* $\mathcal{M}_n(R)$.

Proof. Given the matrix $A = \begin{bmatrix}\mathbf{a}_1 & \mathbf{a}_2 & \dots & \mathbf{a}_m\end{bmatrix}^t$ with each row $\mathbf{a}_j \in R^n$, then

$$AM_\lambda = \begin{bmatrix}\rho_\lambda(\mathbf{a}_1) & \rho_\lambda(\mathbf{a}_2) & \dots & \rho_\lambda(\mathbf{a}_m)\end{bmatrix}^t.$$

As $\rho_\lambda(e_i) = e_{i+1}$ for $i = 1, \dots, n-1$ and $\rho_\lambda(e_n) = \lambda$, it follows that $\mathrm{circ}_\lambda(e_2) = M_\lambda = \mathrm{circ}_\lambda(\rho_\lambda(e_1))$. Therefore, an inductive argument shows that $M_\lambda^k = \mathrm{circ}_\lambda(\rho_\lambda^k(e_1))$, proving the two claims. □

A consequence is,

Corollary 2.7. *With the notation as above,* $M_\lambda^k \in \mathrm{Circ}_{n,\lambda}(R)$ *for all* $k \ge 0$ *and for* $\mathbf{a} = (a_0, a_1, \dots, a_{n-1}) \in R^n$,

$$\mathrm{circ}_\lambda(\mathbf{a}) = \sum_{i=0}^{n-1} a_i M_\lambda^i.$$

Proposition 2.8. *For a finite commutative ring* R, $\mathrm{Circ}_{n,\lambda}(R)$ *is a commutative* R*-subalgebra of* $\mathcal{M}_n(R)$, *the algebra of square matrices of order* n *over the ring* R.

Proof. Since $(\mathrm{Circ}_{n,\lambda}(R), +)$ is an additive subgroup of $\mathcal{M}_n(R)$ containing the identity, it is sufficient to show that $\mathrm{Circ}_{n,\lambda}(R)$ is closed under the usual matrix multiplication. Since for any $\mathbf{a} = (a_0, a_1, \dots, a_{n-1}) \in R^n$, $\mathrm{circ}_\lambda(\mathbf{a})$ is expressed as a linear combination of the elements $\mathrm{circ}_\lambda(e_{i+1})$, $0 \le i \le n-1$, and by linearity, it is enough to show the claim for the elements $\mathrm{circ}_\lambda(e_{i+1})$. However from proposition 2.6, (2) it follows that

$$\mathrm{circ}_\lambda(e_{i+1})\,\mathrm{circ}_\lambda(e_{j+1}) = M_\lambda^i M_\lambda^j = M_\lambda^{i+j},$$

and the claim is proved. □

For a commutative ring R, recall that the polynomial representation of the elements of R^n, $R^n \longrightarrow R[x]$ is the following,

$$\mathbf{a} = (a_0, a_1, \dots, a_{n-1}) \mapsto a(x) = a_0 + a_1 x + \dots + a_{n-1}x^{n-1}.$$

Theorem 2.9. *For* $\lambda = (\lambda_0, \lambda_1, \dots, \lambda_{n-1}) \in R^n$, $\mathrm{Circ}_{n,\lambda}(R)$ *is isomorphic to* $R[x]/\langle x^n - \lambda(x)\rangle$ *as* R*-algebras.*

Proof. Let $\Psi : \mathrm{Circ}_{n,\lambda}(R) \longrightarrow R[x]/\langle x^n - \lambda(x)\rangle$ be given by $\Psi(\mathrm{circ}_\lambda(\mathbf{a})) = a(x) + \langle x^n - \lambda(x)\rangle$, where $\mathbf{a} = (a_0, a_1, \dots, a_{n-1}) \in R^n$. It is straightforward to see that if $\alpha \in R$, $\mathbf{a}, \mathbf{b} \in R^n$, then $\Psi(\alpha\,\mathrm{circ}_\lambda(\mathbf{a}) + \mathrm{circ}_\lambda(\mathbf{b})) = \alpha\Psi(\mathrm{circ}_\lambda(\mathbf{a})) + \Psi(\mathrm{circ}_\lambda(\mathbf{b}))$. On the other hand, from the definition of Ψ and Proposition 2.6,(2) $\Psi(\mathrm{circ}_\lambda(e_{i+1})) = \Psi(M_\lambda^i) = x^i + \langle x^n - \lambda(x)\rangle$, $0 \le i \le n-1$. Then

$$\begin{aligned}\Psi(\mathrm{circ}_\lambda(e_{i+1})\,\mathrm{circ}_\lambda(e_{j+1})) &= \Psi(M_\lambda^{i+j}) \\ &= x^{i+j} + \langle x^n - \lambda(x)\rangle \\ &= \Psi(\mathrm{circ}_\lambda(e_{i+1})\Psi(\mathrm{circ}_\lambda(e_{j+1})),\end{aligned}$$

from which the claim follows by linearity. □

Observe that if $\lambda = (1, 0, \ldots, 0)$, $\mathrm{Circ}_{n,\lambda}(R)$ is the usual circulant matrix over R and Theorem 2.9 gives the well known identification with the ring $R[x]/\langle x^n - 1\rangle$, particularly in the study of cyclic codes over the ring R.

3. λ-VECTOR-CIRCULANT BASED ADDITIVE CODES

In this section R will denote a finite commutative ring unless otherwise indicated. The seminal work [4] on the study of codes with alphabet a finite ring has received the attention of several research groups. These finite rings include chain rings, Galois and Frobenius rings.

An additive code over a finite commutative ring R is a subgroup $\mathcal{C}$ of $(R^n, +)$ ([1], [2]) generated by k rows from a $k \times n$ matrix in $\mathcal{M}_{k\times n}(R)$ which is called the generating matrix. If the generating matrix is of type λ-vector-circulant, the additive code it generates is a λ-vector-circulant based additive code.

Given a ring alphabet R with q elements, an additive code $\mathcal{C}$ with minimum Hamming distance will be denoted by (n, q^k, d) where k indicates the number of generator rows. Recall that the minimum (Hamming) distance of an additive code $\mathcal{C}$ is given by $d_H(\mathcal{C}) = \min_{c\neq \mathbf{0}}\{\mathrm{wt}_H(\mathbf{c}) \mid \mathbf{c} \in \mathcal{C}\}$, by the additivity property, where wt_H denotes the Hamming weight of a codeword, i.e., the number of non-zero components of $\mathbf{c}$, and $\mathbf{0}$ is the zero element of R^n. Note that $\mathcal{C}$ may not be linear over R as it may not be closed under scalar multiplication.

An additive code is said to be half-rate if it is of the form $(n, 2^n)$. We recall the Singleton bound ([6]) for the Hamming distance d_H, in the context of finite commutative rings:

Theorem 3.1 (Singleton Bound)**.** *Let $\mathcal{C}$ be a code of length n over an alphabet of size q with minimum Hamming distance d_H. Then* $\log_q(|\mathcal{C}|) \leq n - d_H + 1$.

We focus on the specific ring $R = \mathbb{F}_2 + u\mathbb{F}_2 = \{0, 1, u, 1 + u \mid u^2 = 0\}$. This is a local chain ring with 4 elements, maximal ideal $\mathfrak{m} = \langle u\rangle$ and residue field $\mathbb{F}_2 = R/\mathfrak{m}$.

As $|R^n| = 2^{2n}$, $|\mathcal{C}| = 2^k$ for some $0 \leq k \leq 2n$. In this case $\mathcal{C}$ is said to be a $(n, 2^k, d)$ code where d is the minimum Hamming distance. In particular, a half-rate additive code over R is one of the form $(n, 2^n, d)$. From the Singleton bound it follows that

$$n \log_4(2) \leq n - d_H + 1 \Rightarrow d_H \leq \left\lfloor \frac{n}{2} \right\rfloor + 1.$$

If the equality is attained the additive code $\mathcal{C}$ is called extremal. Similarly, if $d_H = \left\lfloor \frac{n}{2} \right\rfloor$ the code $\mathcal{C}$ is said to be near-extremal. By means of the software SageMath ([7]) extremal and near-extremal half-rate λ-vector-circulant based additive codes over the ring R for small values of n were obtained (Table 1). Recall that $d_H(\mathcal{C})$ denotes the minimum Hamming distance of the additive code $\mathcal{C}$.

TABLE 1. λ-vector-circulant based codes over R of length n and minimum (Hamming) distance $d_H(\mathcal{C})$ generated from $\mathrm{circ}_\lambda(\mathbf{a})$. Character $*$ indicates the code is near-extremal.

n	λ	$\mathbf{a}$	$d_H(\mathcal{C})$	$\lvert\mathcal{C}\rvert$
3	$(1,0,u)$	$(1,u,0)$	2	8
4	$(1,0,u,u)$	$(1,u,u,0)$	3	16
5	$(1,0,u,1,1)$	$(0,0,1,1+u,1)$	3	32
6$*$	$(1+u,0,1,1+u,0,0)$	$(1,1+u,0,u,1+u,1)$	3	64
6	$(1,0,0,0,u,u)$	$(1+u,0,u,u,u,0)$	4	64
7$*$	$(1+u,0,0,1+u,0,0,1)$	$(u,1+u,u,0,u,0,0)$	3	128
7	$(1+u,0,0,1,0,0,0)$	$(1,0,0,u,0,u,u)$	4	128
8$*$	$(1,u,0,0,1+u,0,0,0)$	$(0,0,1,0,u,0,u,u)$	4	256
8	$(1,0,0,0,0,1,0,1)$	$(1+u,1+u,u,1,u,u,1+u,0)$	5	64
9$*$	$(1,0,0,1+u,0,0,1,0,0)$	$(u,0,0,1+u,1,u,1,u,u)$	4	512
9	$(1,0,0,1,0,0,0,1,0)$	$(0,0,1,1,1+u,1+u,0,1,1)$	5	256
10$*$	$(1,u,u,u,1,0,u,1,1,u)$	$(0,0,0,1,0,0,u,1+u,1+u,1)$	5	256
10	$(1,0,0,1,1,0,1,0,0,1)$	$(0,0,0,1,u,u,1,1+u,0,u)$	6	64

Acknowledgement. The first author was partially supported by Sistema Nacional de Investigadores (SNI), México, and the second author by fellowship No. 764803, Consejo Nacional de Humanidades, Ciencias y Tecnologías (CONAHCYT), México.

REFERENCES

1. Bierbrauer, J. (2012). Cyclic additive codes. J. Algebra 372, 661-672. https://doi.org/10.1016/j.jalgebra.2012.08.031
2. Danielsen L. E., & Parker M. G. (2011). Directed graph representation of half-rate additive codes over $GF(4)$. Designs, Codes and Cryptography 59, 119-130, https://doi.org/10.1007/s10623-010-9469-6
3. Davis P.J. (1979). Circulant Matrices. Wiley-Interscience, N.Y.
4. Hammons, A.R., Kumar P.V., Calderbank, A.R., Sloane, N.J.A., & Solé, P. (1994). The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes. IEEE Transactions on Information Theory 40(2), 301-319, https://doi.org/10.1109/18.312154
5. Jitman, S. (2017). Vector-Circulant Matrices over Finite Fields and Related Codes. Information, 8(3), 82; https://doi.org/10.3390/info8030082
6. Shiromoto K. (2000). Singleton bounds for codes over finite rings. Journal of Algebraic Combinatorics 12, 95-99. https://doi.org/10.1023/A:1008767703006
7. The Sage Developers. SageMath, the Sage Mathematics Software System (Version 10.0), 2023, https://www.sagemath.org.

[1] DEPARTAMENTO DE MATEMÁTICAS, UNIVERSIDAD AUTÓNOMA METROPOLITANA, UNIDAD IZTAPALAPA, 09350 CDMX, MÉXICO.
Email address: htr@xanum.uam.mx

[2] DEPARTAMENTO DE MATEMÁTICAS, UNIVERSIDAD AUTÓNOMA METROPOLITANA, UNIDAD IZTAPALAPA, 09350 CDMX, MÉXICO.
Email address: oczalevaj@gmail.com