DOCTORATE
THESIS MONITORING COMMITTEE PERIODIC EVALUATION REPORT

Student's	
Institute Registered	**Graduate School of Natural and Applied Sciences**
Department	**Mathematics (English)**
Program	**PhD**
Student ID Number	**13565006**
Full Name	**Sümeyra BEDİR**
TMC meeting place-date	
Periodic Evaluation Term	☒ **May - Jun 201…** ☐ **Nov - Dec 201…**
Periodic Evaluation Number	☒ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
THESIS TITLE	**Vectorial Cyclic Codes And Their Structure**
Does the content correspond to the Thesis proposal?	☐ **YES** ☐ **NO**
EVALUATION OF THE THESIS STUDY	☐ **Successful** ☐ **Unsuccessful** ☐ **by unanimious votes** ☐ **by majority of votes**

THESIS MONITORING COMMITTEE MEMBERS			
	Appellation, Full Name	**Department/ University**	**Date-Signature**
Thesis Advisor	**Prof. Dr. İrfan ŞİAP**	**Department of Mathematics/ Yıldız Technical University**	
Committee Member	**Assoc. Prof. Dr. Bayram Ali ERSOY**	**Department of Mathematics/ Yıldız Technical University**	
Committee Member	**Assoc. Prof. Dr. Bahattin YILDIZ**	**Department of Mathematics/ Fatih University**	

Additional Document: Student's Report

NOTE: The thesis committee members who have additional personal remarks may specify them with a report.

1 Introduction (A Brief Summary)

Polycyclic codes over finite fields, first introduced as pseudo-cyclic codes in [17], are shown to be useful in terms of constructing long-length and optimal linear codes directly [3, 7, 11]. Even though it is proven that polycyclic codes correspond to shortened cyclic codes over finite fields, these codes are linear codes different from cyclic or consta-cyclic codes and they enjoy an algebraic structure. This algebraic structure gives a hand to explore this family of linear codes.

Our recent work "Polycyclic codes over finite chain rings" deals with the structure of these codes in the most general way and has been presented in the Proceedings of The International Conference on Coding Theory and Cryptography (ICCC2015).

1.1 Cyclic Codes

Let F be a finite field. A linear code C over F with length n, is a subspace of the vector space F^n. Linear codes, simply denoted with $[n, k, d]$, are identified with their parameters; length(n), dimension(k) and the minimum Hamming distance (d), which is defined as the minimum number of different coordinates between any two codewords of C. C is called a cyclic linear code if whenever $(c_0, c_1, \dots, c_{n-1})$ is in C, so is its cyclic shift $(c_{n-1}, c_0, \dots, c_{n-2})$. So cyclic codes are invariant subspaces of F^n under the transformation which applies cyclic shift to a vector. Each codeword $(c_0, c_1, \dots, c_{n-1})$ is associated to a polynomial $c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ in $F[x]$ and every cyclic code corresponds to an ideal of $F[x]/(x^n - 1)$. The representation matrix for the cyclic shift transformation, denoted by T, is precisely the companion matrix of $x^n - 1$, and any divisor of this polynomial generates a cyclic code over F.

1.2 Constacyclic Codes

For $\alpha \in F$, $\alpha-$constacyclic codes correspond to ideals in $F[x]/(x^n - \alpha)$. As a generalization of cyclic codes, constacyclic codes are invariant under the constacyclic shift; if whenever $(c_0, c_1, \dots, c_{n-1})$ is in C, so is its $\alpha-$constacyclic shift $(\alpha c_{n-1}, c_0, \dots, c_{n-2})$. The transformation for α-constacyclic shift of a vector is represented by the companion matrix of $x^n - \alpha$, which we denote by T_α. Any divisor $g(x)$ of the polynomial $x^n - \alpha$, generates an $\alpha-$ constacyclic code over F.

1.3 Polycyclic Codes

Polycyclicity is the most general case in terms of cyclicity of linear codes. Some authors have called these type of codes as "pseudo-cyclic codes" [17], some as "generalized cyclic codes (GCC)" [10] and some as "polycyclic codes" [11]. There have been many studies on the properties of polycyclic codes [3, 7, 11].

Polycyclic codes correspond to ideals in $F[x]/(f(x))$, for any monic polynomial $f = x^n - v(x)$ with a nonzero constant term. In this case, the companion matrix of f represents the transfomation that corresponds to the polycyclic shift with respect to v, and we denote it by T_v. A polycyclic code generated by a divisor g of f is invariant under T_v, has a generator matrix $g(T_v^{tr})$ and a parity check matrix $h(T_v)$ [7].

We have the following definition for polycyclic codes

Definition 1.1 *A linear code C with length n over a finite field F is called right polycyclic with respect to $v = (v_0, v_1, \ldots, v_{n-1}) \in F^n$ (with the usual correspondence to $v(x) = v_0 + v_1 x + \cdots + v_{n-1}x^{n-1}$) if, whenever $c = (c_0, c_1, \ldots, c_{n-1})$ is in C, so is its v-polycyclic shift $(v_0 c_{n-1}, c_0 + v_1 c_{n-1}, \ldots, c_{n-2} + v_{n-1}c_{n-1})$.*

It is clear that any cyclic code is *polycyclic* with respect to $v = (1, 0, \ldots, 0).(v(x) = 1)$; and any constacyclic code with respect to α, is *polycyclic* with respect to $v = (\alpha, 0, \ldots, 0).(v(x) = \alpha)$.

Consider the following transformation

$$\begin{aligned} \tau_v : \quad F^n &\to F^n \\ (c_0, c_1, \ldots, c_{n-1}) &\mapsto (v_0 c_{n-1}, c_0 + v_1 c_{n-1}, \ldots, c_{n-2} + v_{n-1} c_{n-1}) \end{aligned}$$

It has the following representation matrix as $\tau_v(c) = T_v c$, and T_v is exactly the companion matrix for $f(x) = x^n - v(x)$.

$$T_v = \begin{bmatrix} 0 \cdots \cdots 0 & v_0 \\ 1 \;\; 0 \;\; \cdots 0 & v_1 \\ 0 \;\; 1 \;\; \ddots \vdots & \vdots \\ \vdots \ddots \;\; \ddots 0 & \vdots \\ 0 \cdots \;\; 0 \;\; 1 & v_{n-1} \end{bmatrix}_{nxn}$$

A polycyclic code with respect to v is invariant under τ_v.

The following type of matrices, called "$v-$based vector circulant matrix of c" [9], generate polycyclic codes;

$$G = \begin{bmatrix} c_0 & \cdots & c_{n-1} \\ - & T_v \overrightarrow{c} & - \\ - & T_v^2 \overrightarrow{c} & - \\ & \vdots & \\ - & T_v^{n-1} \overrightarrow{c} & - \end{bmatrix}_{nxn}$$

2 Polycyclic Codes Over Finite Chain Rings

An associative finite ring with unity is called a **chain ring** if its ideals are linearly ordered under inclusion. Finite chain rings are **principal ideal rings**; every ideal of these rings is generated by a single element. They are also **local rings**; they have unique maximal ideals.

While constructing linear codes over finite chain rings, we are going to be dealing with **factorization of polynomials** and we also need a **Euclidean type algorithm**, therefore we make use of the corresponding definitions and theorems.

Let $K = R/M$ be the residue field of a finite chain ring R. A polynomial f in $R[x]$ is called **basic irreducible** if its image μf under the natural projection $\mu : R[x] \longrightarrow K[x]$, is irreducible over $K[x]$. A *primary* polynomial is defined to be a polynomial which generates a primary ideal; an ideal $I \neq R$, for which $xy \in I$ implies $x \in I$ or $y^n \in I$ for some $n \in \mathbb{Z}^+$. A polynomial f in $R[x]$ is called **regular**, if it is not a zero divisor. We have the following equivalent conditions for regular polynomials.

Theorem 2.1 (Theorem XIII.2(c) [14]) *Let $f = a_0 + a_1 x + \cdots a_n x^n$ be a polynomial in $R[x]$. Then the following are equivalent:*

(i) f is regular,

(ii) The ideal $(a_0, a_1, \cdots, a_n) = R$,

(iii) a_i is a unit in R for some i, $0 \leq i \leq n$,

(iv) $\mu f \neq 0$.

Theorem 2.2 (Hensel's Lemma) *Let f be a polynomial in $R[x]$ and $\mu f = \overline{g_1} \cdots \overline{g_n}$ be the factorization of μf over K into pairwise coprime polynomials $\overline{g_1}, \ldots, \overline{g_n}$. Then there exist polynomials $g_1, \ldots, g_n$ in $R[x]$ such that*

(i) $g_1, \ldots, g_n$ are pairwise coprime,

(ii) $\mu g_i = \overline{g_i}$, for all i, $0 \leq i \leq n$,

(iii) $f = g_1 \cdots g_n$.

It is also shown in terms of irreducibilty that for a regular polynomial f, if μf is irreducible in $K[x]$ then f is irreducible in $R[x]$. Moreover if μf has distinct zeros in the algebraic closure of K, then f is irreducible if and only if μf is irreducible [14]. So, we have the following factorization theorem for regular polynomials over R.

Theorem 2.3 (Theorem XIII.11 [14]) *Let f be a regular polynomial in $R[x]$. Then, $f = \delta g_1 \cdots g_n$ where δ is a unit and $g_1, \ldots, g_n$ are pairwise coprime regular primary polynomials. If $f = \beta h_1 \cdots h_m$ is another factorization of f where β is a unit and $h_1, \ldots, h_m$ are pairwise coprime regular primary polynomials, then $m = n$ and $g_i = h_i$ up to reordering.*

As a consequence of this fact, for a **square-free, monic, regular** polynomial f , this factorization into pairwise coprime monic basic irreducible factors is unique up to associates and reordering.

A Euclidean type algorithm also holds as follows:

Theorem 2.4 ([14]) *Let f and g be polynomials in $R[x]$ such that g is regular. Then, there exist polynomials $q, r \in R[x]$ with $f = qg + r$ and* $\deg(r) < \deg(g)$.

2.1 Polycyclic Codes as Invariant Submodules

Let f be a square-free, monic regular polynomial in $R[x]$. And let $f(x) = x^n - v(x) = f_1.f_2.....f_t$ be the unique factorization of f into pairwise coprime, monic, basic irreducible polynomials over the finite chain ring R. Consider the submodules $f_i(T_v)x = 0$, where $x \in R^n$. Denoting $U_i = Ker f_i(\tau_v)$, we give a generalization of the results in [18] and [20] to the polycyclic case as follows

Lemma 2.1 *(i) Each U_i is a free τ_v-invariant submodule of R^n.*

(ii) If W is a τ_v-invariant submodule of R^n and $W_i = W \cap U_i$ for $i = 1, 2, \ldots, t$, then W_i is τ_v-invariant and $W = \bigoplus_{i=1}^{t} W_i$.

(iii) $R^n = \bigoplus_{i=1}^{t} U_i$

(iv) $rank(U_i) = \deg(f_i)$

(v) The minimal polynomial of τ_v over U_i is $f_i(x)$

(vi) U_i is a free minimal τ_v-invariant submodule of R^n

(vii) If U is a free τ_v-invariant submodule of R^n, then U is a direct sum of some minimal free τ_v-invariant submodules U_i of R^n.

Theorem 2.5 *Let C be a linear polycyclic code of length n over R. Then the following facts hold*

(i) $C = \bigoplus_{j=1}^{s} U_{i_j}$ *for some minimal τ_v-invariant submodules of R^n and $rank(C) = \sum_{j=1}^{s} k_{i_j}$ where k_{i_j} is the rank of U_{i_j}*

(ii) $h(x) = f_{i_1}(x).f_{i_2}(x).\dots.f_{i_s}(x)$ *is the minimal polynomial of τ_v over C*

(iii) $rank(h(T_v)) = n - rank(C)$

(iv) $c \in C$ *if and only if* $h(T_v)c = 0$.

If $g(x) = f(x)/h(x)$ is the generating polynomial of a polycyclic code C, then $H = h(T_v)$ is a parity check matrix for C and $G = g(T_v^{tr})$ is a generator matrix for C which gives the vector-circulant matrix of $c = (g_0, g_1, \dots, g_{n-1})$ with respect to v.

Example 2.1 *Let $R = GR(2^2, 3)$ be the Galois ring obtained from the quotient ring $\mathbb{Z}_4[x]/(p(x))$ where $p(x)$ is a basic irreducible polynomial of degree 3 with ξ as a primitive root. And let $f(x) = x^7+3x^6+x^4+3x^3+x+3$. So we have $v(x) = x^6+3x^4+x^3+3x+1$ $v = (1, 3, 0, 1, 3, 0, 1)$ and $f(x)$ has a unique factorization into basic irreducible polynomials g_1, g_2, g_3, g_4 over R as*

$$\begin{aligned} f(x) &= g_1(x)g_2(x)g_3(x)g_4(x) \\ g_1(x) &= (x+3), \\ g_2(x) &= (x^2+3\xi x+1), \\ g_3(x) &= (x^2+(3\xi^2+2)x+1), \\ g_4(x) &= (x^2+(\xi^2+\xi+1)x+1). \end{aligned}$$

We have

$$T_v = \begin{bmatrix} 0&0&0&0&0&0&1 \\ 1&0&0&0&0&0&3 \\ 0&1&0&0&0&0&0 \\ 0&0&1&0&0&0&1 \\ 0&0&0&1&0&0&3 \\ 0&0&0&0&1&0&0 \\ 0&0&0&0&0&1&1 \end{bmatrix}$$

Let C be the right polycyclic code generated by $g_3(x)g_4(x), 2g_3(x)$. We obtain a generator matrix by evaluating $[g_3g_4 + 2g_3](T_v^{tr})$. In standard form we get;

$$
G = \begin{bmatrix} 1\,0\,0\,1 & 0 & 0 & 1 \\ 0\,1\,0\,1 & \xi+1 & \xi^2+1 & 2\xi^2+\xi \\ 0\,0\,1\,\xi & \xi^2+1 & 2\xi^2+\xi & 3 \\ 0\,0\,0\,2 & 0 & 2\xi^2+2\xi+2 & 2\xi^2 \\ 0\,0\,0\,0 & 2 & 2\xi^2 & 2 \end{bmatrix}
$$

and C is a $(7, 4^9 2^6)$ linear code over R.

We have searched over quaternary codes of length up to 29 and found many new codes most of which have better parameters than the known ones. Some of them are given in [7] The codes are constructed with the software Magma and have at least twice the size of the existing linear codes with the same length and same Lee weight in the database [4].

TABLE 1. Some good polycyclic quaternary codes

v	g	*PCCode*	*Size*	*BestAround*	*Size*
$3^3 0 3^3 0 3 0^6$	$3^2 2 1 0^2 3 0 1^2 0^5$	[15, $4^6 2^1$, 8]	8192	[15, $4^6 2^0$, 8]	4096
$3 0 3 0^3 3 0^2 3 0^6$	$3 1 3 1^3 0 3 2 1^2 0 1^2 0^2$	[16, $4^3 2^1$, 12]	128	[16, $4^3 2^0$, 12]	64
$3^2 0 3^2 0^2 3^2 0^2 3 0^5$	$1 0 3 1 0 1 0^2 2^2 3 1 0^5$	[17, $4^6 2^1$, 10]	8192	[17, $4^6 2^0$, 10]	4096
$3 0^2 3^5 0 3 0^2 3^2 0^4$	$1 2 0 2 3 0 3 0^2 1 2 3 2 1 0^4$	[18, $4^5 2^1$, 12]	2048	[18, $4^5 2^0$, 12]	1024
$3^2 0^3 3 0^2 3^2 0 3 0^2 3 0^4$	$3 0 3^2 0^4 1 0 1 0 1^3 0 1^2 0$	[19, $4^2 2^1$, 18]	32	[19, $4^2 2^0$, 18]	16
$3^2 0^6 3 0^{11}$	$1 0^2 2 3^4 1 0 3 2 1^2 2 0 1 0^3$	[20, $4^4 2^1$, 14]	512	[20, $4^4 2^0$, 14]	256
$3^4 0^9 3 0^2 3 0^3$	$3 0 1^3 0 3 0 2 1^2 3 0^2 3^2 2 1 0^2$	[20, $4^3 2^4$, 14]	1024	[20, $4^4 2^0$, 14]	256
$3 0 3^2 0^3 3^3 0^3 3 0 3^2 0^3$	$1^2 0^2 2 1 0^3 2^2 3^2 0 1 0^5$	[20, $4^6 2^1$, 12]	8192	[20, $4^6 2^0$, 12]	4096
$3 0^2 3 0^4 3^3 0^{10}$	$3 1 2 1 2^3 0 2 3 2 3 0 1^2 2 1 0^4$	[21, $4^5 2^1$, 14]	2048	[21, $4^5 2^0$, 14]	1024
$3 0 3 0 3 0^2 3^2 0 3 0^4 3 0^5$	$1^2 0^2 2 1 0^3 2^2 3^2 0 1 0^5$	[21, $4^8 2^1$, 12]	131072	[21, $4^8 2^0$, 12]	65536
$3 0^3 3^4 0^2 3 0 3^3 0^7$	$3 0^2 3 1 3^2 0 3 0^2 2^2 1 0 2 1 0^5$	[22, $4^6 2^1$, 14]	8192	[22, $4^5 2^0$, 14]	1024
$3^2 0^2 3 0 3^3 0^2 3 0^{12}$	$3 0 3 0 1 3 2 3 2 0 2 1 3 2 1 3 0 1 0^6$	[24, $4^7 2^1$, 14]	32768	[24, $4^5 2^0$, 14]	1024
$3^3 0 3 0^3 3 0 3^2 0^{13}$	$3 2 1 2 0^3 1^4 2 3 1 2 3 0^2 3 1 0^5$	[25, $4^6 2^3$, 14]	32768	[25, $4^5 2^0$, 14]	1024
$3 0^5 3 0^5 3 0^{12}$	$1 3 2 0 2 0^2 2 1 0 1 0 1^3 0 2 1 0^7$	[25, $4^8 2^1$, 14]	131072	[25, $4^5 2^0$, 14]	1024
$3^4 0^4 3^2 0^{16}$	$1 0^2 2 0 3^2 0 1^3 0^2 2 1 2 1 2 1^2 0 1 0^4$	[26, $4^5 2^2$, 16]	4096	[26, $4^5 2^0$, 16]	1024
$3^3 0 3^2 0^3 3^2 0^{15}$	$3 0 3 1^3 3^2 2^3 3 1 0^2 1 3 1 2 1^2 0^5$	[26, $4^6 2^1$, 16]	8192	[26, $4^5 2^0$, 16]	1024
$3 0^4 3^2 0^2 3^2 0^2 3 0 3 0 3 0^8$	$1^2 2 3 2^2 0 1 2^2 1 2 0 3 2 3 1 0 2 3^2 1 0^4$	[26, $4^5 2^4$, 16]	16384	[26, $4^5 2^0$, 16]	1024
$3^2 0 3^2 0^3 3 0^3 3 0 3^3 0^9$	$1 3 1 3 2 3 0 1 3 1^3 3 1^4 0^2 1 0^6$	[26, $4^7 2^1$, 16]	32768	[26, $4^5 2^0$, 16]	1024
$3^3 0^3 3 0^{20}$	$3 1^2 2 0 1 2^2 1 3 1 2 1 3^2 2 3 0 1 0 1 0^6$	[27, $4^7 2^5$, 11]	524288	[27, $4^8 2^0$, 11]	65536
$3 0^2 3^5 0^{19}$	$3 1^2 2 3 0^2 1 2 0^2 3 2 1 2 1^2 2 1^2 0^7$	[27, $4^8 2^4$, 11]	1048576	[27, $4^8 2^0$, 11]	65536
$3^5 0 3^2 0 3 0^{17}$	$3 2 3^2 0 2^2 0 3 0 3 2 1 2^2 0^2 1 0^9$	[27, $4^{10} 2^2$, 11]	4194304	[27, $4^8 2^0$, 11]	65536
$3^3 0^{25}$	$1 3 2 1 2 0 3^2 1 0 3 1 3^2 2^3 3 2 1 0^8$	[28, $4^9 2^1$, 14]	524288	[28, $4^7 2^0$, 13]	16384
$3^3 0^3 3 0^{21}$	$1 3 0 2 3^2 0 1^2 2 0 2 1 2^2 1 0 2^2 0 3^2 1 0^5$	[28, $4^6 2^3$, 16]	32768	[28, $4^6 2^0$, 15]	4096
$3^2 0^2 3 0 3^2 0^2 3^3 0^{15}$	$3 0 1 0 1 3 1 0^2 1^3 0 1^2 0 1^2 2 1 0^8$	[28, $4^9 2^2$, 16]	1048576	[28, $4^7 2^0$, 13]	16384
$3 0^2 3 0^{25}$	$3 1 2 1^2 2 3^2 0 2 1 3 0 1 3 1 3 0 2^2 1 0^8$	[29, $4^9 2^3$, 13]	2097152	[29, $4^8 2^0$, 13]	65536

3 Polycyclic Codes with applications to DNA

Polycyclic codes with their structure are useful in many areas of coding theory. One of them is the application of coding theory in DNA computing.

The interest on DNA computing originally was initiated by Adleman where DNA property was used to solve an NP-complete problem [2]. It is also well-known that DNA whenever it reproduces errors may occur and DNA due to its structural properties it can detect such errors and control them. Reproduction and similar activities in DNA take places in a huge amount and this error control capability of the DNA has attracted many researchers in coding theory. In this direction algebraic codes that resemble the DNA structure so called DNA codes are constructed in many aspects and have been studied intensively. The researchers have focused on codes with specific properties (reversible, reversible-complement) and studied their structures ([1, 6, 15, 16, 19, 21]).

In [1], by considering additive codes, especially codes over F_4 (a finite field with four elements) where a very natural one to one correspondence between DNA single bases (Adenine(A), Guanine(G), Cytosine(C), Thymine(T)) and the elements of F_4 are studied. Later, in [15, 16], elements of F_{16} and $F_{4^{2k}}$ are matched to DNA 2-bases and DNA $2k$-bases respectively and codes over these fields with specific properties are studied.

Using the necessary DNA correspondence tables and the map Θ,which resolves the so-called reversibility problem, the following definition and result become the straightforward generalizations of the concepts in [15, 16];

Theorem 3.1 *The polycyclic code generated by a polynomial $g(x)$ is reversible if and only if $g(x)$ is self reciprocal; $g(x) = g^R(x)$.*

Definition 3.1 *Let $g(x)$ be a polynomial over $F_{4^{2k}}$. $g(x)$ is called a polynomial of 4^k-lifted form, if $g(x)$ have the term $a^j x^i$ and $a^{j4^k} x^{deg(g(x))-i}$ for all $i \in \{0, 1, ...\lceil deg(g(x))/2\rceil\}$.*

Theorem 3.2 *Let $g(x)$ be a polynomial of 4^k-lifted form over $F_{4^{2k}}$ with $\deg g(x) = t$. For an arbitrary length n, the spanning set*

$$S_{g(x)} = \{g(x), xg(x), \ldots, x^{n-t-1}g(x)\}$$

generates a polycyclic code C. Then $\Theta(C)$ is a reversible DNA code of length $2kn$.

And, the code generated by the spanning set

$$S_{g(x)} = \{g(x), xg(x), \ldots, x^{n-t-1}g(x), r(x)\}$$

where $r(x) = 1 + x + \cdots + x^{n-1}$, corresponds to a reversible complement DNA code of length $2kn$.

We have obtained reversible DNA codes using polycyclic codes which are optimal codes according to Griesmer bound over $F_{2^{2k}}$.

Example 3.1 *Consider the polynomial* $g(x) = 1 + \omega^{14}x + \omega^{11}x^2 + x^3$ *over* F_{16}*, where* ω *is a root of an irreducible polynomial of degree* 4 *over the prime field* F_2.

$g(x)$ *generates a [7,4,4] optimal polycyclic code which satisfies the Griesmer bound over* F_{16}. *It is also an MDS code. This code corresponds to a reversible DNA code. The generator matrix is as follows:*

$$\begin{pmatrix} 1 & \omega^{14} & \omega^{11} & 1 & 0 & 0 & 0 \\ 0 & 1 & \omega^{14} & \omega^{11} & 1 & 0 & 0 \\ 0 & 0 & 1 & \omega^{14} & \omega^{11} & 1 & 0 \\ 0 & 0 & 0 & 1 & \omega^{14} & \omega^{11} & 1 \end{pmatrix}$$

...

4 Future Work

Vector circulant matrices have various applications in different areas of coding theory. Some of these applications, which we are examining as a continueing work are

- Constructing Recursive MDS Matrices [5]
- Constructing linear codes over Rank Metric and Term Rank Metric Spaces [8]

Another further research objective is to examine the structure of polycyclic codes over some noncommutative rings.

References

[1] T. Abulraub, A. Ghrayeb and X. Nian Zeng, Construction of cyclic codes over $GF(4)$ for DNA computing, J. Franklin Inst., 343 (2006), 448–457.

[2] L. Adleman, Molecular computation of solutions to combinatorial problems, Science, New Series, 266 (1994), 1021–1024.

[3] A. Alahamdi, S. Dougherty, A. Leroy, and P. Sole, On the duality and the direction of polycyclic codes, preprint.

[4] A. Asamov, N. Aydın, The database for $\mathbb{Z}_4$ codes, http://www.asamov.com/Z4Codes/, (2007). accessed at June, 2015.

[5] Augot D., Finiasz M.: Direct construction of recursive MDS diffusion layers using shortened BCH codes, Lecture Notes in Computer Science, vol. 8540, Springer, Berlin (2015).

[6] A. Bayram, E.S. Oztas and I. Siap, Codes over $F_4 + vF_4$ and some DNA applications, Designs, Codes and Cryptography, (2015).

[7] S. Bedir and I. Siap, Polycyclic Quaternary Codes, Proceedings of The International Conference on Coding Theory and Cryptography (ICCC2015), Algeria.

[8] V. V. Gritsenko and A. E . Maevskiy, On a construction of optimal codes in term rank metric via $p(x)$-circulants, 14th International Workshop on Algebraic and Combinatorial Coding Theory, September 7–13, Svetlogorsk (Kaliningrad region), Russia (2014).

[9] S. Jitman, Vector-circulant matrices over finite fields and related codes, arXiv:1408.2059 [math.RA], (2014).

[10] Zhuo-Jun Liu and Dong-Dai Lin, A class of generalized cyclic codes, Acta Math. Appl. Sinica (English Ser.) 16 (2000), no. 1, 53–58.

[11] S.R. Lopez-Permouth, B.R. Parra-Avila, and S. Szabo, Dual generalizations of the concept of cyclicity of codes, Adv. in Math. of Com., (2009), 227–234.

[12] S. R. López-Permouth, H. Özadam, F. Özbudak, and S. Szabo, "Polycyclic codes over Galois rings with applications to repeated-root constacyclic codes," Finite Fields Appl., 19(1):16–38, (2013).

[13] J.L. Massey, Reversible codes, Information and Control, 7 (1964), 369–380.

[14] B. R. McDonald, Finite rings with identity. Marcel Dekker Inc., New York, Pure and Applied Mathematics, Vol. 28, (1974).

[15] E.S. Oztas and I. Siap, Lifted polynomials over F_{16} and their applications to DNA Codes, Filomat, 27 (2013), 459–466.

[16] E.S. Oztas and I. Siap, On a generalization of lifted polynomials over finite fields and their applications to DNA codes, Int. J. Comput. Math., 92 (2015), 1976–1988.

[17] W. W. Peterson and E. J. Jr Weldon, Error Correcting codes: second edition, MIT Press, (1972).

[18] D. Radkova, A.J. Van Zanten, Constacyclic codes as invariant subspaces, Linear Algebra and its Applications, 430 (2009), pp. 855-864.

[19] I. Siap, T. Abulraub and A. Ghrayeb, Cyclic DNA codes over the ring $F_2[u]/(u^2 - 1)$ based on the deletion distance, J. Franklin Inst., 346 (2009), 731–740.

[20] M. Wu, Free cyclic codes as invariant submodules over finite chain rings, International Mathematical Forum, 8-37(2013), pp. 1835 - 1838.

[21] B. Yildiz and I. Siap, Cyclic codes over $F_2[u]/(u^4 - 1)$ and applications to DNA codes, Comput. Math. Appl., 63 (2012), 1169–1176.