ISSN (Online) : 2454 -7190 **ISSN (Print) 0973-8975**

Codes of Polynomial Type

Mohammed Sabiri

Faculty of Science and Technology, Department of Mathematics, Moulay Ismail University, Errachidia, Morocco

https://doi.org/10.26782/jmcms.2019.04.00028

Abstract:

In this work we try to introduce the concept of codes of polynomial type and polynomial codes that are built over the ring A[X]/A[X]f(X).It should be noted that for particular cases of f we will find some classic codes for example cyclic codes, constacyclic codes, So the study of these codes is a generalization of linear codes.

Keywords: Cyclic codes, dual code, Polynomial code, principal polynomial code, codes of polynomial type.

I. Introduction

Linear codes have been an interesting topic of both mathematics and engineering for decades. They are prominently used in consumer electronics, data transmission technologies, broadcast systems, and computer applications. Linear codes are codes that use linear algebra. Linear algebra in turn is built on two basic elements, the matrix and the vector (Klein, 2013). Linear codes provides concepts that are crucial to many areas of computer science, including graphics, image processing, cryptography, information retrieval and web search.

Cyclic codes are the most studied of all codes, since they are easy to encode, and include the important family of BCH codes (Adamek, 1991). Furthermore they are building blocks for many other codes.

The classical approaches to the study and construction of cyclic codes are those based on the generator matrix, the generator polynomial and the idempotent (van Lint, 1973). The objective of this paper is to develop another approach. Fundamental theory of this approach will be developed, and will be employed to construct a new family of codes.

II. LINEAR CODES OVER FINITE FIELDS

II.i Linear Codes

Definition 2.1. Let $\mathbb{K}$ be a finite field of order q. A linear code C of length n over $\mathbb{K}$ is a subspace of the $\mathbb{K}$ -space $\mathbb{K}^n$. If more C has dimension k , then C is said a [n; k]-code.

Definition 2.2. The generator matrix G for a linear code C is a k by n matrix for which the rows are basis of C.

Table 1: Linear code over $\mathbb{z}/2\mathbb{z}$.

C	000	011	101	110

If G is a generator matrix for C, then

$C = \{aG\ I\ a \in \mathbb{K}^k\}$ (van Lint, 1999).

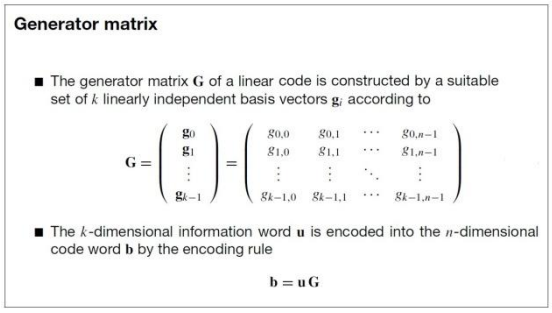

Figure 1: Generator matrix of a linear code B(n,k)

The information word u = (u_0;$u_{\ldots}$;u_{k-1}) is encoded according to the matrix-vector multiplication b = uG:

All M = q^K code words b €B(n;k) can be generated by this rule. Owing to this property, the linear code B(n;k) is completely defined with the help of the generator matrix G (Neubauer et al., 2007).

II.ii Cyclic Codes

Definition 2.3. Let T be a cyclic shift operator T: $\mathbb{K}^n \rightarrow \mathbb{K}^n$, which transforms v = ($v_0$,$v_1$, …,$v_{n-1}$) into vT = ($v_{n-1}$,$v_0$,$v_1$, …,$v_{n-2}$). A linear code C is called the cyclic code of length n if it is invariant under T.

To get an algebraic description, we associate

with the vector c = (c_0, $c_{1,\ldots,}$ c_{n-1}) in $\mathbb{K}^n$ the polynomial c(x) = c_o + c_1x + ::: + $c_{n-1}x^{n-1}$

(Williams and Sloane, 1981).

We shall use the following notation. If $\mathbb{K}$ is a field,

$\mathbb{K}[x]$ denotes the set of polynomials in x with coefficients from $\mathbb{k}$ In fact, $\mathbb{K}[x]$ is a ring.

The ring $R_n = \mathbb{K}[x] / (x^n - 1)$. For our purposes another ring is more important than $\mathbb{k}[x]$ This is the ring $R_n = \mathbb{K}[x]]/ (x^n - 1)$, consisting of the residue classes of K[x] modulo $x^n - 1$. Each polynomial of degree $\leq$ n-1 belongs to a different residue class, and we take this polynomial as representing its residue class.

Thus we can say that c(x) belongs to R_n. R_n is a vector space of dimension n over $\mathbb{K}$.

Table 2: Cyclic code of length 3 over $\mathbb{z}/3\mathbb{z}$.

C	000	110	101	011
	0	$1+x$	$1+x^2$	$x+x^2$

Definition 2.5. A cyclic code of length n over $\mathbb{k}$ Is an ideal of R_n.

III. LINEAR CODES OVER RINGS

We assume that all rings in this paper are commutative with identity.

Definition 3.1. Let A be a ring. A linear code C

of length n over A is a submodule of the free module A^n. And the elements of C are called the words of the code. If more C is a sub A- free module of rank k, then C is said a [n; k]-code of A and k is called the rank of the code C.

Table 4: C a code of length 2 over $A = \mathbb{Z}/4\mathbb{Z}$.

00	10	20	30	02	12	22	32

As in the case of A is a field, it defines the inner

product of two elements a = (a_1,…,a_n) and b =

(b_1,..;b_n) of An by:

$a.b = \sum_{i=1}^{n} a_i b_i$,

The operations being carried out in A, this inner product

allows to define a notion of duality on A and it

was:

Definition 3.2. (dual Code) Let C be a linear code on A, then

$C^{\perp} = \{a \in C \ \ \mathrm{I} : (\forall\, b \in C)\ (a.b = 0)\}$,

is a linear code of length n on A called the dual code of the code C.

Definition 3.3. A linear code C of length n over A is cyclic if :

a- C is linear,

b- Any cyclic shift of a codeword of C is

a codeword of C, i.e., if $(c_o,c_1,\ldots,c_{n-1}) \in$ C then

$(c_{n-1},c_o;c_1,\ldots,c_{n-2}) \in$ C.

As is customary, A_n will denote the ring $\frac{\mathrm{A[X]}}{X^n-1}$

and the elements of A_n will be identified with polynomials over A of degree $\leq$ n-1. Also, an n-tuple $(c_o,c_1,\ldots, c_{n-1})$ in An will be identified with the element $(c_o + c_1x + ::: + c_{n-1}x^{n-1})$ of $A_n = \frac{\mathrm{A[X]}}{X^n-1}$ Using this identification, it is easy to see that the cyclic A-codes correspond precisely to the ideals of A_n (Greferath, 1997).

IV. Structures of A [X]-Modules and Codes of Polynomial Type

Theorem 4.1. Let A be a ring with identity and M an left A-module.

The following conditions are equivalent:

i) M can have a structure of A[X]-module which extends

that of the A-module M.

ii) There is an endomorphism T of the left A-module (M;+).

Proof. If M has a structure of left A[X]-module

which extends that of the A-module M then the application

$\widetilde{X}$: M $\rightarrow$M

m $\rightarrow \widetilde{X}$ (m) = X.m

is an endomorphism of the left A-module M.

Conversely, if there is an T endomorphism of the left A-module then T sets an action of A[X]-module on M which extends that of the A -module M by:

A[X] × M $\rightarrow$M

$\left(\sum_{i=0}^{n} a_i\ X^i, m\right) \longrightarrow \sum_{i=0}^{n} a_i\ T^i(m)$

Example 4.2. Let M be a free A-module of

rank n, B = (e_1,…,e_n) a basis of M on A and

an endomorphism T of ($_A$M;+), then the structure of A[X]-module on M from an endomorphism T can be defined as follows:

Let D = $(d_{i\,j})_{1\leq i,\, j\leq n}$ the matrix of T relatively at the

base B, that is to say

$$T(e_i) = \sum_{j=1}^{n} d_{ji}\ e_i$$

For $m = \sum_{j=1}^{n} x_j\ e_j$ Let's ask $C_m = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ \vdots \\ x_n \end{pmatrix}$

and for

$$C = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ \vdots \\ c_n \end{pmatrix} \in M_{(n,1)}(A)$$ Let

$V_C := \sum_{j=1}^{n} c_j\ e_i$. Then $X.m = V_{DC_m}$.

Example 4.3. Let A be a commutative ring with

identity and

$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \quad \in A[X]$, so it is well known that:

1. M = A[X]/A[X] f (X) is a free A-module of rank n.

2. M has a structure of A[X]-module defined by:

$$A[X] \times M \longrightarrow M$$

(P(X), Q(X) + A[X] f (X))⟶

P(X)Q(X)+A[X]f (X).

This structure is the one that extends the structure of the A-module M and such that:

X.(Q(X) + A[X] f (X)) =XQ(X)+A[X] f (X).

3. The A[X] structure of M module defined in

2) is the one that extends that of the A-module

A[X]/A[X] f (X) and associated to the endomorphism T from the A-module M defined by T(Q(X)+A[X] f (X)) = XQ(X)+A[X]f(X)

Furthermore, in B = (1,X,…,X^{n-1}) the base of the

free A-module M we have:

If $T(e_i) = \sum_{j=1}^{n} c_{ji}\ e_j$

such that $e_i \in B$ then

D = (c_{ij}) =

$$C_f = \begin{pmatrix} 1 & 0 & \cdots & 0 & -a_0 \\ 0 & 0 & & 0 & -a_1 \\ \vdots & 1 & \ddots & \vdots & \\ 0 & 0 & & 0 & 0 \\ 0 & 0 & \cdots & 0 & -a_{n-1} \end{pmatrix} \in M_n(A)$$

is the companion matrix of f (X), this matrix is often noted C_f.

4. M = A[X]/A[X] f(X) is a commutative ring with

identity whose multiplication is defined by:

$$M \times M \longrightarrow M$$

(P(X) + A[X]f(X), Q(X) + A[X]f(X)) ⟶

P(X)Q(X)+A[X] f(X).

In addition we have the following important

lemma which is easily verifiable

Lemma 4.4. Let N be a subset of A[X]/A[X]f(X).

So we have:

N is a sub A[X]-module of A[X]/A[X] f (X) if and only if N is an ideal of the ring A[X]/A[X] f (X).

Proof. If I is an ideal of the ring de A[X]/A[X] f(X)

then:

for all P(X) ∈A[X] and all Q(X)+A[X]f(X) ∈ I:

(P(X) + A[X]f(X))(Q(X) + A[X] f (X)) =

P(X)Q(X)+A[X] f (X)

= P(X)(Q(X)+A[X] f (X)) ∈ I.

Conversely, if N is a sub A[X]-module of

A[X]/A[X] f (X) then:

For all P(X)+A[X]f(X) ∈ A[X]/A[X] f (X) and

for all Q(X)+A[X] f (X) ∈ N:

P(X)(Q(X)+A[X]f(X)) = P(X)Q(X)+A[X]f(X)

= (P(X)+A[X] f(X))(Q(X)+A[X]f(X)) ∈ I.

4.1 Linear Transformation Associated a Polynomial

Let A be a commutative ring with identity. An important example of endomorphisms of the A-module A^n is the one associated to the given monic polynomial $f(X) \in A[X]$ of degree n. This endomorphism is defined as follows:

Let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \quad \in A[X]$..

For $(c_1,\ldots,c_n) \in M_{(1,n)}(A)$ let:

$V_{(c1\ldots cn)} = (c_1,\ldots,c_n) \in A^n$

$t_{(c1\ldots cn)}$ the transposed matrix of $(c_1\ldots c_n)$.

Then

T_f: $A^n \rightarrow A^n$

$(c_1,\ldots,c_n) \rightarrow T_f(c_1,\ldots,c_n) := V_{Cf(t(c1\ldots cn))}$.

is an un endomorphism of A-module An called linear transformation associated to the unitary polynomialf (X).

where

$$\mathcal{C}_f = \begin{pmatrix} 1 & 0 & \cdots & 0 & -a_0 \\ 0 & 0 & & 0 & -a_1 \\ \vdots & 1 & \ddots & \vdots & \\ 0 & 0 & & 0 & 0 \\ 0 & 0 & \cdots & 0 & -a_{n-1} \end{pmatrix} \in M_n(A)$$

Is the companion matrix of f (X).

Then

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & -a_0 \\ 0 & 0 & & 0 & -a_1 \\ \vdots & 1 & \ddots & \vdots & \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & & 0 & -a_{n-1} \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ c_3 \\ \vdots \\ c_n \end{pmatrix}$$

$$= \begin{pmatrix} -a_0 c_n \\ c_1 - a_1 c_n \\ \vdots \\ \vdots \\ c_{n-1} - a_{n-1} c_n \end{pmatrix}$$

$$= \begin{pmatrix} 0 \\ c_1 \\ \vdots \\ \vdots \\ c_{n-1} \end{pmatrix} - c_n \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ \vdots \\ a_{n-1} \end{pmatrix}$$

So : T_f: $A^n \rightarrow A^n$

$(c_1,\ldots,c_n) \rightarrow T_f(c_1,\ldots,c_n) := V_{Cf(t(c1\ldots cn))} =$

$(-a_0c_n - c_1,\ldots,c_{n-1} - a_{n-1}c_n)$

Consequence 4.5. : A^n is a A[X]- module for action defined by

$$X.(c_1, \ldots, c_n) = T_f(c_1, \ldots, c_n)$$

and extended by linearity at A[X].

Examples 4.6. :

1. If $f(X) = X^n - 1$ then:

$$C_f = \begin{pmatrix} 1 & 0 & \cdots & 0 & 1 \\ 0 & 0 & & 0 & 0 \\ \vdots & 1 & \ddots & \vdots & \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & & 0 & 0 \end{pmatrix} \in M_n(A)$$

And

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & 1 \\ 0 & 0 & & 0 & 0 \\ \vdots & 1 & \ddots & \vdots & \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & & 0 & 0 \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ c_3 \\ \vdots \\ c_n \end{pmatrix}$$

$$= \begin{pmatrix} c_n \\ c_1 \\ \vdots \\ \vdots \\ c_{n-1} \end{pmatrix}$$

$$T_f : A^n \longrightarrow A^n$$

$$(c_1 , \dots , c_n) \longrightarrow V_{\,C_f(t_{(c_1 ,\dots,c_n)})} = (c_n , \dots , c_{n-1}).$$

A^n is a A[X]- module for action

defined by:

$$X.(c_1 , \dots , c_n) = T_f(c_n , \dots , c_{n-1})$$

and extended by linearity at A[X].

2. If $f(X) = X^n - \lambda$ then:

$$C_f = \begin{pmatrix} 1 & 0 & \cdots & 0 & \lambda \\ 0 & 0 & & 0 & 0 \\ \vdots & 1 & \ddots & \vdots & \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & & 0 & 0 \end{pmatrix} \in M_n(A)$$

And

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & \lambda \\ 0 & 0 & & 0 & 0 \\ \vdots & 1 & \ddots & \vdots & \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & & 0 & 0 \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ c_3 \\ \vdots \\ c_n \end{pmatrix}$$

$$= \begin{pmatrix} \lambda c_n \\ c_1 \\ \vdots \\ \vdots \\ c_{n-1} \end{pmatrix}$$

$$T_f : A^n \longrightarrow A^n$$

$$(c_1 , \dots , c_n) \longrightarrow V_{\,C_f(t_{(c_1 ,\dots,c_n)})} = (\lambda c_n , \dots , c_{n-1}).$$

A^n is a A[X]- module for action

defined by:

$$X.(c_1, \dots, c_n) = T_f(c_n, \dots, c_{n-1})$$

and extended by linearity at A[X].

4.2 Codes of Polynmial Type

Let A be a ring with identity

and $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in A[X]$ Then:

$$\phi_f : A^n \longrightarrow A[X]/A[X]f(X)$$

$v=(v_0,\dots,v_{n-1}) \rightarrow \sum_{i=0}^{n-1} v_i X^i + A[X]f(X)$

is an isomorphism of A-modules. ϕ_f shows how

to translate the results of A[X]/A[X] f (X) to A^n , if n = deg (f(X)).

More precisely, the action of the ring A[X] on

$A[X]/A[X]f(X)$ is translated in action of A[X] on A^n by the extension by linearity at A[X] of

$X.(c_1,\dots,c_n) = T_f(c_1,\dots,c_n)$, of so that ϕ_f becomes an isomorphism of A[X]-modules.

Definition 4.7. Let f (X) be a monic polynomial of A[X].

A polynomial code (resp principal polynomial) of

length n on A is an ideal (resp principal ideal) of

$A[X]/A[X]f(X)$.

A code of polynomial type (resp of principal polynomial type) of length n on A is the inverse image of a polynomial code (resp. principal polynomial) of length n over A, by the application ϕ_f described in the proposal above.

Consequences 4.8. :

Cyclic codes and constacyclic codes are examples of codes of polynomial type. Indeed the cyclic codes of length n correspond to the polynomial codes of the case where $f(X) = X^n - 1$, and the constacyclic codes

of length n correspond to the polynomial codes of the case where $f(X) = X^n - \lambda$ for a $\lambda \in A$

5 Codes of Polynmial Type andTheir Generator Matrices

Let f (X) be a monic polynomial of A[X] and

C(X) a principal polynomial code of

A[X]/A[X] f(X).

Then there exists:

g(X) = $\sum_{i=0}^{r} giX^{I} \in A[X]$ such that C(X) =

A[X]g(X)/A[X] f (X)

In the following we suppose that g is monic:

Theorem 5.1. Let C(X) be a principal polynmial

code of A[X]/A[X] f (X), then with the notations above

we have :

(a) ∃ h(X) ∈ A[X] such that f (X) = g(X)h(X).

-The C code of polynomial type corresponding to C(X) := A[X]g(X)=A[X] f (X) is of dimension n-r where deg(f (X)) = n and deg(g(X)) = r.

(b) If v := $(c_0,c_1,\ldots,c_{n-1}) \in C$ then $T_f(v) \in C$.

(c) The rows of a matrix generating C are given by $(T_f)^k(g_0,g_1,\ldots,g_r)$ for $1 \leq k \leq n-r$.

Proof. (a) Let's show that B is a base of C(X)

where B = $\{g(X),Xg(X),\ldots,X^{n-r-1}g(X)\}$.

The Euclidean division f (X) = Q(X)g(X) + r(X)

with deg(r(X)) < deg(g(X)) shows that r(X) = 0 and therefore g(X)/f (X).

The family B is free and generator. Indeed Let's first show that B is a generator.

Let P ∈ C(X) =< g(X) > then ∃ Q(X) ∈ A[X] I P(X) = Q(X)g(X) Or Q(X) = $\sum_{i=0} aiX^{I}$ hence P(X) = Q(X)g(X) = $\sum_{i=0} a_i X^i g(X)$ So just

show that: $X^{j}{}_{j \geq n-r} g(X) = \sum_{i=0}^{n-r-1} \lambda_i X^i g(X)$

We have $X^{j}g(X) = f(X)q(X)+r(X)$ I d°r(X) < n. (1)

As g(X)/ f (X) then g(X)/r(X).

Therefore ∃ $r_1(X) \in A[X]$ such that $r(X) = g(X)r_1(X)$.

Since $r(X) \neq 0$ then $\deg(r(X)) = \deg(g(X)) + \deg(r_1(X)) < n$.

As a result, $\deg(r_1(X)) < n-\deg(g(X)) = n-r = k$.

From where $r_1(X) = \sum_{i<n-r} b_i X^i \Longrightarrow \overline{X^{j}g(X)} = r(X)$ [f (X)].

So what $\overline{X^{j}g(X)} = \sum_{i=0}^{n-r-1} \overline{X^{j}g(X)}$ Which shows that B is a generator family.

Let $(a_0; a_1,..., a_{n-r-1}) \in A^n$ I $\sum_{i=0}^{n-r-1} a_i X^j$ g(x) = 0.

$\overline{a_0 g(X) + \cdots + a_{n-r-1} X^{n-r-1} g(X)=\bar{0}}$

From where f (x)/ a_0g(X) +,…+a_{k-1}g(X) =0.

which is possible unless a_0g(X) +,…+a_{k-1}g(X) = 0.

Since g(X) $\neq 0$ we have $a_i = 0\ \forall i \in \{0 \ldots, k-1\}$, so B is free.

Finally B is a base.

(b) The advanced relationship is the exact translation of the fact that C(X) is an ideal A[X]- module A[X]/A[X] f (X) or it's the translation of the makes C(X) stable by multiplying by X in A[X]/A[X] f (X).

(c) Indeed, B = (g(X) + A[X] f(X), ...,X^{n-r-1}g(X) + A[X] f (X)) is a base of the ideal C(X). Hence ϕ^{-1}(B) is a base of the code C.

Or ϕ^{-1}(B) = ((g_0, g_1,…,g_r),…,$(T_f)^{n-r-1}$(g_0, g_1,…,g_r)

Examples 5.2. 1.If $f(X) = X^n - 1$ and f (X) = g(X)h(X).

a) A code C of polynmial type of A^n is a cyclic code of length n over A.

(b) From the above theorem becomes:

v := (c_0,c_1 ,…,c_{n-1}) ∈ C then (c_{n-1} ,c_0,c_1 ,…,c_{n-2}) ∈ C.

(b) Then expresses the condition of cyclicity for a code C.

2. If f (X) = X^n-λ and f (X) = g(X)h(X).

- a) A code C of polynmial type is a constacyclic code of length n over A.

-b) From the above theorem becomes:

If v := (c_0,c_1 ,…,c_{n-1}) ∈ C then (λc_{n-1} ,c_0, ,…,c_{n-2}) ∈ C.

(b) then expresses the condition of constacyclicity for a code C.

Remark 5.3. :

The (b) property of the above theorem:

"If v := (c_0,c_1,…,c_{n-1}) ∈ C then T_f (v)∈ C"

characterizes the codes of polynomial type defined from the monic polynomial f (X) of A[X].

5.1 Codes of Polynomial Type and Their Control

What is the control matrix of such a code that corresponds to the ideal

C(X) = A[X]g(X)/A[X] f (X) ?.

Lemma 5.4. If C(X) = A[X]g(X)/A[X] f (X) then

for all h(X) ∈ A[X] such that f (X) = g(X)h(X) we have :

C(X) = $\mathrm{Ann}_{A[X]/A[X]\,f(X)}$ (A[X]h(X)/A[X] f (X)) :

(Annulator in A[X]/A[X] f (X) of

A[X]h(X)/A[X] f (X)).

Proof. Let c ∈ C(X) then there exists P(X) ∈ A[X] such that:

c = P(X)g(X)+A[X] f (X) and then

(P(X)g(X) + A[X] f (X))(Q(X)h(X) + A[X] f (X))

= (P(X)g(X)Q(X)h(X) + A[X] f(X)) = A[X] f (X):

For a polynomial $h(X) = X^s + h_{s-1}X^{s-1} + \cdots + h_0 \in A[X]$.

Let $h^*(X) = 1 + h_{s-1}X^1 + \cdots + h_0X^{s-1} \in A[X]$.

Proposition 5.5.

If C(X) = A[X]g(X)/A[X]($X^n - 1$) so for

h(X) ∈ A[X] such that (X^n -1) =g(X)h(X)

we have :

$C(X)^{\perp}$ = A[X] $h^*(X)$/A[X]($X^n - 1$)

Proof. The advanced arguments in the case where A is a field are still valid in this case where A is a ring.

VI. Conclusion

In this work we have studied the codes of polynomial type, it is natural to ask the following question is it possible to build unconventional codes and exploit these codes in applications for example cryptography, knowing that for choices of f, we can build good codes.

VII. Acknoledgement

The author is greatly indebted to the referee for his/her useful suggestions.

References

I. Adamek, J. (1991). Foundations of coding. Interscience, Prague.

II. Greferath, M. (1997). Cyclic codes over finite rings. Discrete Mathematics 177, University of Duisburg.

III. Klein, P. N. (2013). Coding the Matrix: Linear Algebra through Computer Science Applications. Newtonian Press, Brown, first edition.

IV. Neubauer, A., Freudenberger, J., and Kuhn, V. (2007). Coding Theory - Algorithms, Architectures, and Applications.Wiley-Interscience, Germany.

V. Springer, Eindhoven University, third edition.

VI. van Lint, J. (1973). Coding Theory. Springer-Verlag Berlin Heidelberg, London, 2nd edition.

VII. van Lint, J. (1999). Introduction to Coding Theory.

VIII. Williams, F. M. and Sloane, N. J. A. (1981). The theory of error-corecting codes. Mathematical Library, North-Holland, third edition.