Uluslararası İleri Doğa Bilimleri ve Mühendislik Araştırmaları Dergisi
Sayı 8, S. 708-715, 11, 2024

Araştırma Makalesi

IJANSER
https://as-proceeding.com/index.php/ijanser
ISSN:2980-0811

International Journal of Advanced Natural Sciences and Engineering Researches
Volume 8, pp. 708-715, 11, 2024

Research Article

Applications of Fixed Minimum Distance Codes with Generators in Standard Form

Mustafa ÖZKAN[1*]

[1] *Mathematics and life Science Department / Faculty of Education, Trakya University, Turkiye*

[*] *mustafaozkan@trakya.edu.tr*

(Received: 11 December 2024, Accepted: 29 December 2024)

(5th International Conference on Scientific and Academic Research ICSAR 2024, December 23-24, 2024)

ATIF/REFERENCE: ÖZKAN, M. (2024). Applications of Fixed Minimum Distance Codes with Generators in Standard Form. *International Journal of Advanced Natural Sciences and Engineering Researches*, 8(11), 708-715.

Abstract – In this study, basic information about algebra and coding theory is mentioned. Afterwards, generator matrices that produce a linear code are written in standard form, a classification of code types corresponding to codes with parameters $(n+1,4^n,2)$ of the codes produced by these matrices and examples are presented. It has been generalized using the same ring as in my work in References [6].

Keywords – *Mathematical Modeling of Communication, Coding Theory, Linear Codes, Generator Matrices.*

I. EXTENDED SUMMARY AND INTRODUCTION

In the study, a code set that provides the Group property has been created. $R = \mathbb{F}_2 + u\mathbb{F}_2$ The code set has been defined with generator matrices consisting of a ring of elements and having certain properties. Previously, codes with generator matrices have been discussed in the study numbered [6]. This study has been generalized, and certain generalizations have been made regarding the parameters of the codes by writing the generator matrices in standard form and information has been presented about their parameters. Results have been obtained about the generator matrices used to create the elements of the code set and the codes that have the properties of the matrices that include zero and those that do not include zero in the standard form. It has been shown which type of block code the generator

matrices specify according to their types. These results have been presented by reaching a general judgment.

These statements have been reached 4^1 , 4^2 ve 4^3 after the applications of block codes have been shown. The limitations of these applications have been determined and their suitability has been determined.

II. BASIC KNOWLEDGE

In this section, basic information is presented first.

2.1 Definition: $\mathbb{F}$ when the given conditions are met on which the defined addition and subtraction operations are performed, it is called a field.

i. $\mathbb{F}$ is a commutative ring.
ii. $\mathbb{F}$ every element of has a multiplicative inverse except zero.

2.3 Definition: A finite field is a field $\mathbb{F}$, if its elements have finite elements $\mathbb{F}$.

2.4 Definition: In coding theory, an error-correcting code that converts blocks of information of a certain length into blocks of code of a fixed length is called a block code.

2.5 Definition: Since the code words in a block code form a collection group, this code is called a group code.

2.6 Definition: The basic criteria that define the properties and performance of a code are called the parameters of the code.

These parameters are usually (n, M, d) expressed in a ternary notation as [n, k, d] if the code is a linear code. The definitions of these parameters are:

Code Length (n): Indicates the length of the code word (code blocks). A code word consists of n symbols.

Code Words **(** M **):** Each code word indicates the number of code words it contains.

Minimum Hamming distance (d **):** It expresses the minimum Hamming distance of the code. Minimum Hamming distance determines the error detection and correction capabilities of the code and represents the least bit difference between any two different code words.

(k): is the number of elements in the base of the linear code. It is also expressed as the number of rows of the generator matrix

Hamming distance determines the error detection and correction capacity of the code . Code length and number of code words determines the coding efficiency and capacity of the code.

2.7 Definition: Let the elements IF_q^n of $x = (x_1, x_2, ..., x_n)$, $y = (y_1, y_2, ..., y_n)$ be given.

x and y The function defined d as the number of distinct components $d(x, y) = \left| \{ i \mid x_i \neq y_i , i = 1,2,...,n \} \right|$ of the Hamming distance is called.

C is a linear code of $n\_$ length $d(C) = \min\{ d(x, y) \mid x \neq y , x, y \in C \}$ is called the minimum distance of the code C.

2.8 Definition: C a $[n, k]\_$ code is called if the minimum distance of a vector space $d(C) = d$ is $k\_$ dimensional subspace C of the vector space . If indicated by C a linear $[n, k, d]\_$ code is called.

2.9 Definition: Let IF_q^n any vector space $x = (x_1, x_2, ..., x_n)$ element of weight..

It is defined as $w(x) = \left| \{ i \mid x_i \neq 0, i = 1,2,...,n , x_i \in IF_q \} \right|$.

C is a linear code $w(C) = \min\{ \quad w(x) \quad | \quad x_i \neq 0 \, , \, x \in C \quad \}$

is called the weight of the C code.

2.10 Proposition [8] : Each for $x, y \in IF_q^n$ **,** thus $d(x, y) = w(x - y)$.

2.11 Theorem: Let C is a linear code of $n\_$ length, then $d(C) = w(C)$.

Evidence: $x = (x_1, x_2, ..., x_n)$, $y = (y_1, y_2, ..., y_n) \in C$ including

$d(C) = \min\{ \; d(x, y) \; | \; x \neq y \, , x, y \in C \; \}$ because it is

$\Rightarrow \exists \, x, y \in C$ for $d(C) = d(x, y) = w(x - y)$

$\geq \min\{ \quad w(x) \quad | \quad x_i \neq 0 \, , \, x \in C \quad \} = w(C)$ is found.

$\therefore \quad d(C) \geq w(C)$.

$w(C) = \min\{ \quad w(x) \quad | \quad x_i \neq 0 \, , \, x \in C \quad \}$ because it is $w(C) = w(x)$ for $x \in C$.

$\therefore \; \exists \, x \in C$ for $w(C) = w(x) = w(x - 0) = d(x, 0) \geq \min\{ \; d(x, y) \; | \; x \neq y \, , x, y \in C \; \} = d(C)$. It is seen that.

$\therefore \quad w(C) \geq d(C)$ is .

$\therefore \; w(C) = d(C)$ It is possible.

From the above theorem, m it is concluded that in order to determine the minimum distance of $\binom{m}{2} = \frac{1}{2}.m.(m-1)$ a linear code with elements, C it will be sufficient to look at the weight of the code word instead of making comparisons $m - 1$.

2.12 Definition: Let C be a code of $n\_$ length on the ring $R = IF_2 + u\, IF_2$.

The Lee weight of the codeword $c = (c_0, c_1, ..., c_{n-1}) \in C$ where $w_L(c) = \sum_{i=0}^{n-1} w_L(c_i)$ is defined in the form $w_L(0) = 0$, $w_L(1) = 1$, $w_L(1 + u) = 1$, $w_L(u) = 2$.

$d_L(c, d) = w_L(c - d)$ every for $c, d \in R^n$ The function defined d_L is called as Lee distance . The minimum Lee distance of a $C \subseteq R^n$ code is defined as $d_L(C)) = \min\{ \, w_L(c) \, | \, c \in C \setminus \{0\}\}$.

The weight function defined here is given for the ring $R = \mathbb{F}_2 + u\mathbb{F}_2, (u^2 = 0)$. The weight function is defined differently in different rings.

2.13 Definition: Let C be a linear $[n, k]\_$ code. The matrix of type C obtained $k \times n$ by using the one element in the base of k is called the generating matrix of the code and is denoted by G.

2.14 Example: On IF_2, $S = \{ (0,1,1), (1,0,1) \}$

a base of code $C=\{(0,0,0),(0,1,1),(1,0,1),(1,1,0)\}$. Since $G=\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}_{2\times 3}$ the matrix is the generating matrix of C. This $[3,2,2]_$parameter of C code on IF_2 .

2.15 Example: Let $C=\{(0,0,...,0),(1,1,...,1),...,(q-1,q-1,...,q-1)\}\subseteq IF_q^n$ be an $q_$ary code of $n\_$ length. Since code C has a bas , it is $S=\{(1,1,...,1)\}$ a code $[n,1,n]_$parameter with a generating matrix $G=[1\,1\,...\,1]_{1\times n}$.

III. GROUP CODE FORMATION

3.1 Definition: A binary block (a,b)-code has the coding function E :$(F_2)^a \rightarrow (F_2)^b$

A binary block (a,b)-code, decoding in function ; D :$(F_2)^b \rightarrow (F_2)^a$

The images of E are called code words.

3.2 Example : In the ring $R=\mathbb{F}_2+u\mathbb{F}_2$, for $u^2=0$.

Table 1.1 which provides the closure property according to the addition operation shown in the table.

+	0	1	u	1+u
0	0	1	u	1 +u
1	1	0	1+u	u
u	u	1+u	0	1
1+u	1+u	u	1	0

Table 2.2 that the closure property is provided according to the multiplication operation

×	0	1	u	1+u
0	0	0	0	0
1	0	1	u	u
u	0	u	0	u
1+u	0	1+u	u	1

Elements of tables in $R=\mathbb{F}_2+u\mathbb{F}_2$ is codewords of a code of the ring R =$\{0,1,u,1+u\}$.

3.3 Definition [3]: A q- ary (n, m, 2t+1) _ code.

$m\{\binom{n}{0}+\binom{n}{1}(q-1)+\ldots+\binom{n}{t}(q-1)^t\}\leq q^n$

inequality is provided.

The above definition R is given for the boundary ring.

$R = \mathbb{F}_2 + u\mathbb{F}_2$, $u^2 = 0$. It is a 4-element ring and not a field. However, it can be said that a 4-element field is isomorphic to a ring. Therefore, $R = \mathbb{F}_2 + u\mathbb{F}_2$ can correspond our 4-element ring to a 4-element field.

3.4 Definition : One q- ary $(n, m, 2t+1)$_for code

$m.\left\{ \binom{n}{0} + \binom{n}{1}.(q-1) + \ldots + \binom{n}{t}.(q-1)^t \right\} = q^n$ This code is called perfect code.

3.5 Example: A q-ary $(n, 2, n)$_ code is an perfect code.

3.6 Theorem : On$R = \mathbb{F}_2 + u\mathbb{F}_2$, $u^2 = 0$ for $a_1, a_2, a_3, \ldots, a_n \in R$ defined as , specifies a code with an n-row generator matrix 4^n-element Group code.

4^1 Blocky generator matrix→ $G_1 = [1 \quad a_1]$

4^2 Blocky generator matrix → $G_2 = \begin{bmatrix} 1 & 0 & a_1 \\ 0 & 1 & a_2 \end{bmatrix}$

4^3Blocky generator matrix → $G_3 = \begin{bmatrix} 1 & 0 & 0 & a_1 \\ 0 & 1 & 0 & a_2 \\ 0 & 0 & 1 & a_3 \end{bmatrix}$

.

.

4^nBlocky generator matrix→ $G_n = \begin{bmatrix} 1 & \cdots & 0 & a_1 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & a_n \end{bmatrix}$.

It is stated this way.

3.7 Theorem : $R = \mathbb{F}_2 + u\mathbb{F}_2$, $u^2 = 0$ için $a_1, a_2, a_3, \ldots, a_n \in R$ and $x_1, x_2, x_3, \ldots, x_n \in R$ whereas $\begin{bmatrix} 1 & \cdots & 0 & a_1 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & a_n \end{bmatrix}$. Generator matrices of type $4^n$are a block code and a group code with elements.

$C_n = [x_1 \quad x_2 \quad x_3 \cdots \quad x_n].\begin{bmatrix} 1 & \cdots & 0 & a_1 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & a_n \end{bmatrix}$

$= [x_1 \quad x_2 \quad x_3 \quad \ldots \quad x_n \quad a_1x_1 + a_2x_2 + a_3x_3 + \cdots x_n]$

It is written in the format.

3.8. Theorem 2.5: Parameters of code words formed in ring $R = \mathbb{F}_2 + u\mathbb{F}_2$ ve $u^2 = 0$:

Parameter of C_1 code words with 4^1 Blocks generated by G_1;
in the form

$$a_1 = 0, C_1 - (2,4,1)$$
$$a_1 \neq 0, C_1 - (2,4,2)$$

Parameter of C_2 code words with 4^2 Blocks generated by G_2;
in the form

$$\exists\, a_1, a_2 = 0, C_2 - (3,16,1)$$
$$\forall\, a_1, a_2 \neq 0, C_2 - (3,16,2)$$

Parameter of C_3 code words with 4^3 Blocks generated by G_3;
in the form

$$\exists a_1, a_2, a_3 = 0, C_3 - (4,64,1)$$
$$\forall\, a_1, a_2, a_3 \neq 0, C_3 - (4,64,2)$$

$$\vdots$$

Parameter of C_n code words with 4^n Blocks generated by G_n;
in the form

$$\exists a_1, a_2, a_3, \dots, a_n = 0, C_n - (n+1, 4^n, 1)$$
$$\forall\, a_1, a_2, a_3, \dots, a_n \neq 0, C_n - (n+1, 4^n, 2)$$

IV. Applications of Fixed Minimum Distance Codes

4.1 Application:

- $G_{1.1} = [1 \quad 0], [x].[1 \quad 0] = [x \quad 0]$

$C_{1.1} = \{(0,0), (1,0), (u,0), (1+u,0)\}$

$C_{1.1}$ is possible a code with (2,4,1)- parameters.

4.2 Application:

- $G_{1.4} = [1 \quad 1+u], [x].[1 \quad 1+u]$
  $= [x \quad x+xu]$

$C_{1.4} = \{(0,0), (1,1+u), (u,u), (1+u,1)\}$

$C_{1.4}$ is possible a code with (2,4,2)- parameters.

4.3 Application:

- $G_{2.1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, [x \quad y].\begin{bmatrix} 1 & 0 & a \\ 0 & 1 & b \end{bmatrix} = [x \quad y \quad 0]$

$C_{2.1}$=$\{(0,0,0), (0,1,0), (O,u,0), (0,1+u,0), (1,0,0), (1,1,0), (1,u,0)(1,1+u,0), (u,0,0), (u,1,0), (u,u,0), (u,1+u,0), (1+u,0,0), (1+u,1,0), (1+u,u,0), (1+u,1+u,0)\}$

$C_{2.1}$ is possible a code with (3,16,1)- parameters.

4.4 Application:

- $G_{2.7} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & u \end{bmatrix}, [x \quad y] . \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & u \end{bmatrix} = [x \quad y \quad x+uy]$

$C_{2.7} = \{(0,0,0), (0,1,u), (0,u,0), (0,1+u,u), (1,0,1)(1,u,1), (1,1+u,1+u), (1,1,1+u), (u,0,u), (u,1,0), (u,u,u), (u,1+u,0), (1+u,0,1+u), (1+u,1,1), (1+u,u,1+u), (1+u,1+u,1)\}$

$C_{2.7}$ is possible a code with (3,16,2)- parameters.

4.5 Application:

- $G_{3.3} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}, C_{3.3} = [x \quad y \quad z]. \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} = [x \quad y \quad z \quad z]$

$C_{3.3} = \{(0,0,0,0)(0,0,1,1), (0,0,u,u), (0,0,1+u,1+u), (0,1,0,0), (0,1,1,1), (0,1,u,u)(0,1,1+u,1+u), (0,u,0,0)(0,u,1,1), (o,u,u,u), (0,u,1+u,1+u), (0,1+u,0,0), (0,1+u,1,1), (0,1+u,u,u), (0,1+u,1+u,1+u), (1,0,0,0), (1,0,1,1), (1,0,u,u), (1,0,1+u,1+u), (1,1,0,0), (1,1,1,1), (1,1,u,u), (1,1,1+u,1+u), (1,u,0,0), (1,u,1,1), (1,u,u,u), (1,u,1+u,1+u), (1,1+u,0,0)(1,1+u,1,1), (1,1+u,u,u), (1,1+u,1+u,1+u), (u,0,0,0), (u,0,1,1), (u,0,u,u), (u,0,1+u,1+u), (u,1,0,0), (u,1,1,1), (u,1,u,u), (u,0,1+u,1+u), (u,u,0,0), (u,u,1,1), (u,u,u,u), (u,u,1+u,1+u), (u,1+u,0,0), (u,1+u,1,1), (u,1+u,u,u), (u,1+u,1+u,1+u), (1+u,0,0,0), (1+u,0,1,1), (1+u,0,u,u), (1+u,0,1+u,1+u), (1+u,1,0,0), (1+u,1,1,1), (1+u,1,u,u), (1+u,1,1+u,1+u), (1+u,u,0,0), (1+u,u,1,1), (1+u,u,u,u), (1+u,u,1+u,1+u), (1+u,1+u,0,0), (1+u,1+u,1,1), (1+u,1+u,u,u), (1+u,1+u,1+u,1+u)\}$

$C_{3.3}$ is possible a code with (4,64,1)- parameters.

4.6 Application:

- $G_{3.6} = \begin{bmatrix} 1 & 0 & 0 & u \\ 0 & 1 & 0 & u \\ 0 & 0 & 1 & u \end{bmatrix},$

$$C_{3.6} = [x \quad y \quad z]. \begin{bmatrix} 1 & 0 & 0 & u \\ 0 & 1 & 0 & u \\ 0 & 0 & 1 & u \end{bmatrix} = [x \quad y \quad z \quad ux + uy + uz]$$

$C_{3.6} = \{(0,0,0,0)(0,0,1,u), (0,0,u,0), (0,0,1+u,u), (0,1,0,u), (0,1,1,0), (0,1,u,u), (0,1,1+u,0), (0,u,0,0), (0,u,1,u), (0,u,u,0), (0,u,1+u,u), (0,+u,0,u), (0,1+u,1,0), (0,1+u,u,u), (0,1+u,1+u,0), (1,0,0,1), (1,0,1,0), (1,0,u,u), (1,0,1+u,0), (1,1,0,0), (1,1,1,u), (1,1,u,0), (1,1,1+u,u), (1,u,0,u), (1,u,1,0), (1,u,u,u), (1,u,1+u,0), (1,1+u,0,0), (1,1+u,u,0), (1,1+u,1,u), (1,1+u,1+u,u), (u,0,0,0), (u,0,1,u), (u,0,u,0), (u,0,1+u,u), (u,1,0,u), (u,1,1,0), (u,1,u,u), (u,1,1+u,0), (u,u,0,0), (u,u,1,u), (u,u,u,0), (u,u,1+u,u), (u,1+u,0,u), (u,1+u,1,0), (u,1+u,u,u), (u,1+u,1+u,0), (1+u,0,0,u), (1+u,0,1,u), (1+u,0,u,u), (1+u,0,1+u,0), (1+u,1,0,0), (1+u,1,1,u), (1+u,1,u,0), (1+u,1,1+u,u), (1+u,u,0,u), (1+u,u,1,0), (1+u,u,u,u), (1+u,u,1+u,0), (1+u,1+u,0,0), (1+u,1+u,1,u), (1+u,1+u,u,0), (1+u,1+u,1+u,u)\}$

$C_{3.6}$ is possible a code with (4,64,2)- parameters.

4.7 Example:

Parameter of C_1 code words with 4^1 Blocks generated by G_1;

$$a_1 = 0\,, \quad C_1 \ -(2,4,1)$$
$$a_1 \neq 0\,, \quad C_1 \ -(2,4,2)$$

$4 \cdot \left\{\binom{2}{0}\right\} \leq 4^2$ inequality $4 \leq 4^2$occurs and the limit is provided.

4.8 Example:

Parameter of C_2 code words with 4^2 Blocks generated by G_2;

$$\exists\, a_1, a_2 = 0\,, \quad C_2 - (3,16,1)$$
$$\forall\, a_1, a_2 \neq 0\,, \quad C_2 - (3,16,2)$$

$16 \cdot \left\{\binom{3}{0}\right\} \leq 4^3$ from inequality $4^2 \leq 4^3$happens and the limit is provided .

4.8 Example:

Parameter of C_3 code words with 4^3 Blocks generated by G_3;

$$\exists a_1, a_2, a_3 = 0\,, \quad C_3 - (4, 64, 1)$$
$$\forall\, a_1, a_2, a_3 \neq 0\,, \quad C_3 - (4, 64, 2)$$

$64\left\{\binom{4}{0}\right\} \leq 4^4$ from inequality $4^3 \leq 4^4$happens and the limit is achieved.

4.9 Conclusion: If we make a general judgment about the group code parameters in our study with these examples;

Parameter of C_n code words with 4^n Blocks generated by G_n;

$$\exists a_1, a_2, a_3, \ldots, a_n = 0\,, \quad C_n - (n+1, 4^n, 1)$$
$$\forall\, a_1, a_2, a_3, \ldots, a_n \neq 0\,, \quad C_n - (n+1,\ 4^n, 2)$$

$4^n \cdot \left\{\binom{4^{n+1}}{0}\right\} \leq 4^{n+1}$ from inequality $4^n \leq 4^{n+1}$happens and the limit is achieved.

REFERENCES

[1] Bose , R.C. and Ray- Chaudhuri , D.K. , *On a Class of Error Correcting Binary Group Codes* . Information Control, 3: 68-79, 1960.

[2] Delsarte , P. , *Bilinear Forms Over A Finite Field , With Applications To Coding Theory* . Journal of Combinatorial Theory A, 25: 226–241, 1978.

[3] Lemmermeyer F. , Error-correcting Codes , 2005.

[4] Lin , S. , Xing , C., *Coding Theory -A first course* CambridgeUniversity , 2004 .

[5] Loidreau , P. , *A Welch-Berlekamp Like algorithm for decoding Gabiduline codes* . WWC, 36-45, 2005.

[6] Ozkan, M. and Ozturk, B. , *Certain Rings and Group Codes* . Journal of New Results in Engineering and Natural Science , (8), 25-30,2018.

[7] Pless , V. , *Introduction to the Theory of Error-Correcting Codes* , 1989.

[8] Roman S. , *Coding and Information Theory* . Graduate Text in Mathematics , Springer Verlag , 1992.

[9] Shannon , C.E. , *A Mathematical Theory of Communication* . Bell Sys . tech . J. , pp.379-423 Part 1; pp . 623-656 Part 2, 1948.

[10] Huffman W.C., Pless V. , *Fundamentals of Error Correcting Codes* , Cambridge, 2003.