On Some Properties of Extended Binary Golay [24, 12, 8] Code Using MATLAB

N. S. Darkunde, S. P. Basude, and M. S. Wavare

Abstract The main aim of this paper is to study various properties of extended binary Golay [24, 12, 8] code, when we know its generator matrix. Using MATLAB, we can study syndrome decoding, weight of a codeword, error correction and error detection of extended binary Golay [24, 12, 8] code.

Keywords Linear code · Generator matrix · Parity check matrix · Extended binary golay code · Syndrome decoding

1 Introduction

In the late 1940s Claude Shannon was developing information theory and coding as a mathematical model for communication. In mathematical sciences and electronics engineering, a binary Golay code is a type of linear error-correcting code used in digital communications. The binary Golay code, along with the ternary Golay code, are named in honour of Marcel J. E. Golay whose 1949 paper [1] introducing them has been called, by E. R. Berlekamp, the "best single published page" in coding theory. There are two closely related binary Golay codes. The extended binary Golay code encodes 12 bits of data in a 24-bit word in such a way that any 3-bit errors can be corrected or any 7-bit errors can be detected.

The other, the perfect binary Golay code, has codewords of length 23 and is obtained from the extended binary Golay code by deleting one coordinate position. In standard coding notation the codes have parameters [24, 12, 8] and [23, 12, 7], corresponding to the length of the codewords, the dimension of the code, and the minimum Hamming distance between two codewords, respectively [2, 3]. In [4, 5], algorithmic approach for error correction have been studied for few codes. In this

N. S. Darkunde (✉)
School of Mathematical Sciences, SRTM University, Nanded, Maharashtra, India

S. P. Basude
SRTM University, Nanded, Maharashtra, India

M. S. Wavare
Department of Mathematics, Rajarshi Shahu Mahavidyalaya, Latur, Maharashtra, India

P. M. Pawar et al. (eds.), *Techno-Societal 2020*,
https://doi.org/10.1007/978-3-030-69921-5_71

paper, we are going to study some properties of extended binary Golay [24, 12, 8] code.

2 Preliminaries

2.1 Linear Codes [6]

Let Fq denote the finite field with q elements, where q is some power of a prime. A linear $[n, k]_q$—code is a k-dimensional subspace of F_q^n. The parameters n and k are referred to as the length and dimension of the corresponding code.

Example The subset C = {000, 001, 010, 011} of vector space F_2^3 is $[3, 2]_2$ linear code. Similarly, C = {0000, 1100, 2200, 0001, 0002, 1101, 1102, 2201, 2202} is $[4, 2]_3$ linear code.

2.2 Hamming Distance and Hamming Weight [7]

Let $x, y \in F_q^n$, The Hamming distance from x to y, denoted by $d(x, y)$, is defined to be the number of places at which x and y differ.

Example Consider $x = 01010$,$y = 01101$, $z = 11101$ in F_2^5, Then$d(x, y) = 3$,$d(x, z) = 4$. For any $x \in F_q^n$, the support of$x$, denoted by supp(x), is defined to be the set of nonzero coordinates in $x = (x_1,x_{2,}x_{3,\ldots,}x_n)$, that is $supp(x) = \{i : x_i \neq 0\}$.

For a $[n, k]_q$ code C containing at least two words, the nonnegative integer given by $\min\{d(x, y) : x, y \in C, x \neq y\}$ is called minimum distance of C. It is denoted by $d(C)$.

Example For a code C = {0000, 1000, 0100, 1100} in F_2^4, we see that$d(C) = 1$.

Definition 1 [8] Let u be a positive integer. A code C is u -error-detecting if, whenever a codeword incurs at least one but at most u errors, the resulting word is not a codeword.

A code is exactly u-error-detecting if it is u-error-detecting but not $(u + 1)$ error-detecting.

Example Consider C = {000000, 000111, 111222} $\subseteq$ F_2^6. This code is 2-error-detecting, because changing any codeword in one or two positions does not result in another codeword. In fact, C is exactly 2-error-detecting, as changing each of the last three positions of 000000 to 1 will result in the codeword 000111 (so C is not 3-error-detecting).

Theorem 1 [8] A code C is u -error-detecting if and only if $d(C) \geq u + 1$, that is, a code with distance d is an exactly $(d - 1)$-error-detecting code.

Definition 2 [8] Let v be a positive integer. A code C is v -error-correcting if minimum distance decoding is able to correct v or fewer errors, assuming that the incomplete decoding rule is used. A code C is exactly v-error-correcting if it is v -error-correcting but not $(v + 1)$-error-correcting.

Example Consider $C = \{000, 111\}$ in F_2^3. It is easy to see that, C is 1-error-correcting.

Theorem 2 [8] A code C is v -error-correcting if and only if $d(C) \geq 2v + 1$, that is a code with distance d is an exactly $\lfloor (d - 1)/2 \rfloor$-error correcting code, where $\lfloor x \rfloor$ denote the greatest integer less than or equal to x.

Definition 3 (*Dual Code*). [8] Given a $[n, k]_q$ code C in F_q^n, the subspace
$C^{\perp} = \{x = (x_{1,} x_{2,} x_{3,\ldots,} x_n) \in F_q^n : x.c = 0$ for all $c = (c_1, c_2, \ldots, c_n) \in C\}$,
We have following properties of C and $C^{\perp}$

1. $|C| = q^{\dim(C)}$, i.e$\dim(C) = log_q |C|$;
2. $C^{\perp}$ is a linear code and $\dim(C) + \dim\left(C^{\perp}\right) = n$;
3. $(C^{\perp})^{\perp} = C$.

2.3 *Generator Matrix and Parity-Check Matrix*

Definition 4 [7] A matrix G of order $k \times n$ is said to be the generator matrix for a $[n, k]_q$ code C, if its rows form basis for C.

Definition 5 [7] A parity-check matrix H for a code C is a generator matrix for $C^{\perp}$.

2.4 *Binary Extended Golay [24, 12, 8] Code*

Let $G = (I_{12}|A)$, where I_{12} is a 12×12 identity matrix and A is a 12×12 matrix given by

$$A = \begin{bmatrix} 100011111001 \\ 111010101010 \\ 101111100100 \\ 101110010011 \\ 011111001001 \\ 011100100111 \\ 110101010101 \\ 010010011111 \\ 011001111100 \\ 100100111110 \\ 010111110010 \\ 101001001111 \end{bmatrix}$$

The binary linear code generated by matrix G is called extended binary Golay [24, 12, 8] code.

2.5 Syndrome Decoding [8]

An efficiency of decoding technique works well, when length n of a given code is small, but it can take a more time when, n is very large, so this time can be saved by using the syndrome to identify the coset from which the word is taken. In [8], the procedure of syndrome decoding have been demonstrated.

Step 1: Let w be received word in the transmission and for this received word w, first compute the syndrome of w denoted by Syn(w) which is given by, $syn(w) = wH^T$, where H, is parity check matrix of a given code.

Step 2: After constructing Syndrome look up table, we will find the coset leader u next to the syn $(w) = syn(u)$.

Step 3: Finally decode the received word w as $v = w - u$.

Now, let us study the properties of extended binary Golay [24,12,8] code using MATLAB [9].

2.6 MATLAB Program for Syndrome Decoding Using Extended Binary Golay [24, 12, 8] Code

```
%Extended Golay Code

n = 24; k = 12; %Length and Dimension

clc % Clearscreen

I = eye(12); % Identity matrix of order 12
```

```
A = [1 0 0 0 1 1 1 1 1 0 0 1;
1 1 1 0 1 0 1 0 1 0 1 0;
1 0 1 1 1 1 1 0 0 1 0 0;
1 0 1 1 1 0 0 1 0 0 1 1;
0 1 1 1 1 1 0 0 1 0 0 1;
0 1 1 1 0 0 1 0 0 1 1 1;
1 1 0 1 0 1 0 1 0 1 0 1;
0 1 0 0 1 0 0 1 1 1 1 1;
0 1 1 0 0 1 1 1 1 1 0 0;
1 0 0 1 0 0 1 1 1 1 1 0;
0 1 0 1 1 1 1 1 0 0 1 0;
1 0 1 0 0 1 0 0 1 1 1 1];
G = [I A] % Generator matrix of extended Golay code
H = mod([−A' eye(12)],2) % Denote H as a parity Check Matrix for extended Golay Code
d = gfweight(G) % Distance of Code
slt = syndtable(H); % Produce Syndrome look up table.
w = [1 1 0 1 0 1 0 1 0 1 0 1 1 1 0 0 0 0 0 1 1 0 1 0] % Message received
syndrome = rem(w * H', 2);
syndrome_de = bi2de(syndrome,'left-msb'); % Convert to decimal.
disp(['Syndrome = ',num2str(syndrome_de),' (decimal),',num2str(syndrome),' (binary)'])
corrvect = slt(1 + syndrome_de,:) % Correction vector
% Now compute the corrected codeword.
correctedcode = rem(corrvect + w,2)
G =
Columns 1 through 13
1 0 0 0 0 0 0 0 0 0 0 0 1
0 1 0 0 0 0 0 0 0 0 0 0 1
0 0 1 0 0 0 0 0 0 0 0 0 1
0 0 0 1 0 0 0 0 0 0 0 0 1
```

0 0 0 0 1 0 0 0 0 0 0 0 0

0 0 0 0 0 1 0 0 0 0 0 0 0

0 0 0 0 0 0 1 0 0 0 0 0 1

0 0 0 0 0 0 0 1 0 0 0 0 0

0 0 0 0 0 0 0 0 1 0 0 0 0

0 0 0 0 0 0 0 0 0 1 0 0 1

0 0 0 0 0 0 0 0 0 0 1 0 0

0 0 0 0 0 0 0 0 0 0 0 1 1

Columns 14 through 24

0 0 0 1 1 1 1 1 0 0 1

1 1 0 1 0 1 0 1 0 1 0

0 1 1 1 1 1 0 0 1 0 0

0 1 1 1 0 0 1 0 0 1 1

1 1 1 1 1 0 0 1 0 0 1

1 1 1 0 0 1 0 0 1 1 1

1 0 1 0 1 0 1 0 1 0 1

1 0 0 1 0 0 1 1 1 1 1

1 1 0 0 1 1 1 1 1 0 0

0 0 1 0 0 1 1 1 1 1 0

1 0 1 1 1 1 1 0 0 1 0

0 1 0 0 1 0 0 1 1 1 1

H =

Columns 1 through 13

1 1 1 1 0 0 1 0 0 1 0 1 1

0 1 0 0 1 1 1 1 1 0 1 0 0

0 1 1 1 1 1 0 0 1 0 0 1 0

0 0 1 1 1 1 1 0 0 1 1 0 0

1 1 1 1 1 0 0 1 0 0 1 0 0

1 0 1 0 1 0 1 0 1 0 1 1 0

1 1 1 0 0 1 0 0 1 1 1 0 0

1 0 0 1 0 0 1 1 1 1 1 0 0

1 1 0 0 1 0 0 1 1 1 0 1 0

0 0 1 0 0 1 1 1 1 1 0 1 0

0 1 0 1 0 1 0 1 0 1 1 1 0

1 0 0 1 1 1 1 1 0 0 0 1 0

Columns 14 through 24

0 0 0 0 0 0 0 0 0 0 0

1 0 0 0 0 0 0 0 0 0 0

0 1 0 0 0 0 0 0 0 0 0

0 0 1 0 0 0 0 0 0 0 0

0 0 0 1 0 0 0 0 0 0 0

0 0 0 0 1 0 0 0 0 0 0

0 0 0 0 0 1 0 0 0 0 0

0 0 0 0 0 0 1 0 0 0 0

0 0 0 0 0 0 0 1 0 0 0

0 0 0 0 0 0 0 0 1 0 0

0 0 0 0 0 0 0 0 0 1 0

0 0 0 0 0 0 0 0 0 0 1

d = 8

Single-error patterns loaded in decoding table. 4071 rows remaining.

2-error patterns loaded. 3795 rows remaining.

3-error patterns loaded. 1771 rows remaining.

4-error patterns loaded. 0 rows remaining.

w =

Columns 1 through 13

1 1 0 1 0 1 0 1 0 1 0 1 1

Columns 14 through 24

1 0 0 0 0 0 1 1 0 1 0

Syndrome = 275 (decimal), 0 0 0 1 0 0 0 1 0 0 1 1 (binary)

corrvect =

```
Columns 1 through 13
1 0 0 0 0 0 1 1 0 0 0 0 0
Columns 14 through 24
0 0 0 0 0 1 0 0 0 0 0
Corrected code =
Columns 1 through 13
0 1 0 1 0 1 1 0 0 1 0 1 1
Columns 14 through 24
1 0 0 0 0 1 1 1 0 1 0
```

2.7 MATLAB Program for Encoding Message Using Extended Binary Golay [24, 12, 8] Code

```
% Matlab Programme for Encoding of the information message
n = 24; k = 12; %Length and Dimension
clc % Clearscreen
I = eye(12); % Identity matrix of order 12
A = [1 0 0 0 1 1 1 1 1 0 0 1;
1 1 1 0 1 0 1 0 1 0 1 0;
1 0 1 1 1 1 1 0 0 1 0 0;
1 0 1 1 1 0 0 1 0 0 1 1;
0 1 1 1 1 1 0 0 1 0 0 1;
0 1 1 1 0 0 1 0 0 1 1 1;
1 1 0 1 0 1 0 1 0 1 0 1;
0 1 0 0 1 0 0 1 1 1 1 1;
0 1 1 0 0 1 1 1 1 1 0 0;
1 0 0 1 0 0 1 1 1 1 1 0;
0 1 0 1 1 1 1 1 0 0 1 0;
1 0 1 0 0 1 0 0 1 1 1 1];
G = [I A] % Generator matrix of extended Golay code
```

H = mod([−A' eye(12)],2) % Denote H as a parity Check Matrix for extended Golay Code

u = input('Enter the message bit of length 12 for which you want to encode using extended Golay Code = ')% input message of length 12

v = mod(u*G,2) % Encoding of message u

Synv = mod(v*H',2) % Syndrome of encoded message

G =

Columns 1 through 13

1 0 0 0 0 0 0 0 0 0 0 0 1

0 1 0 0 0 0 0 0 0 0 0 0 1

0 0 1 0 0 0 0 0 0 0 0 0 1

0 0 0 1 0 0 0 0 0 0 0 0 1

0 0 0 0 1 0 0 0 0 0 0 0 0

0 0 0 0 0 1 0 0 0 0 0 0 0

0 0 0 0 0 0 1 0 0 0 0 0 1

0 0 0 0 0 0 0 1 0 0 0 0 0

0 0 0 0 0 0 0 0 1 0 0 0 0

0 0 0 0 0 0 0 0 0 1 0 0 1

0 0 0 0 0 0 0 0 0 0 1 0 0

0 0 0 0 0 0 0 0 0 0 0 1 1

Columns 14 through 24

0 0 0 1 1 1 1 1 0 0 1

1 1 0 1 0 1 0 1 0 1 0

0 1 1 1 1 1 0 0 1 0 0

0 1 1 1 0 0 1 0 0 1 1

1 1 1 1 1 0 0 1 0 0 1

1 1 1 0 0 1 0 0 1 1 1

1 0 1 0 1 0 1 0 1 0 1

1 0 0 1 0 0 1 1 1 1 1

1 1 0 0 1 1 1 1 1 0 0

0 0 1 0 0 1 1 1 1 1 0

1 0 1 1 1 1 1 0 0 1 0

0 1 0 0 1 0 0 1 1 1 1

H =

Columns 1 through 13

1 1 1 1 0 0 1 0 0 1 0 1 1

0 1 0 0 1 1 1 1 1 0 1 0 0

0 1 1 1 1 1 0 0 1 0 0 1 0

0 0 1 1 1 1 1 0 0 1 1 0 0

1 1 1 1 1 0 0 1 0 0 1 0 0

1 0 1 0 1 0 1 0 1 0 1 1 0

1 1 1 0 0 1 0 0 1 1 1 0 0

1 0 0 1 0 0 1 1 1 1 1 0 0

1 1 0 0 1 0 0 1 1 1 0 1 0

0 0 1 0 0 1 1 1 1 1 0 1 0

0 1 0 1 0 1 0 1 0 1 1 1 0

1 0 0 1 1 1 1 1 0 0 0 1 0

Columns 14 through 24

0 0 0 0 0 0 0 0 0 0 0

1 0 0 0 0 0 0 0 0 0 0

0 1 0 0 0 0 0 0 0 0 0

0 0 1 0 0 0 0 0 0 0 0

0 0 0 1 0 0 0 0 0 0 0

0 0 0 0 1 0 0 0 0 0 0

0 0 0 0 0 1 0 0 0 0 0

0 0 0 0 0 0 1 0 0 0 0

0 0 0 0 0 0 0 1 0 0 0

0 0 0 0 0 0 0 0 1 0 0

0 0 0 0 0 0 0 0 0 1 0

0 0 0 0 0 0 0 0 0 0 1

Enter the message bit of length 12 for which you want to encode using

Golay Code = [1 0 1 1 0 0 1 0 1 0 1 0]

u = 1 0 1 1 0 0 1 0 1 0 1 0

v =

Columns 1 through 13

1 0 1 1 0 0 1 0 1 0 1 0 0

Columns 14 through 24

1 1 0 0 1 0 1 0 1 0 1

Synv = 0 0 0 0 0 0 0 0 0 0 0 0

3 Conclusion

Once we know the generator matrix of any linear code, using MATLAB we can have many of the things that can be discussed. In this paper, we have studied extended binary Golay [24, 12, 8] code with the help of MATLAB. The parity check matrix in standard form for extended binary Golay [24, 12, 8] code is calculated and using it, syndrome of a particular codeword is calculated. We have encoded the message and decoded it correctly by using MATLAB. Using MATLAB, it has been verified that, the distance of an extended binary Golay [24, 12, 8] code is 8 and it is 3-error-correcting code.

References

1. Golay MJ (1949) Notes on digital coding. Proc IEEE 37:657
2. Lee HP, Chang CH, Chu SI (2013) High-speed decoding of the binary golay code. J Appl Res Technol 11(3):331–337
3. Reed IS, Yin X, Truong TK, Holmes JK (1990) Decoding the (24, 12, 8) Golay code. IEE Proc E (Comput Digit Tech) 137(3):202–206
4. Patil AR, Darkunde NS (2019) Algorithmic approach for error-correcting capability and decoding of linear codes arising from algebraic geometry. Springer, Information and Communication Technology for Competitive Strategies, pp 509–517
5. Patil AR, Darkunde NS (2017) On some error-correcting linear codes. Asian J Math Comput Res 56–62
6. Huffman WC, Pless V (2010) Fundamentals of error-correcting codes. Cambridge University Press
7. MacWilliams FJ, Sloane NJA (1977) The theory of error-correcting codes. Elsevier
8. Ling S, Xing C (2004) Coding theory-a first course, 1st edn. Cambridge University Press
9. Pratap R (2017) Getting started with MATLAB: a quick introduction for scientists and engineers, 7e. Oxford University Press