General Letters in Mathematics Vol. 2, No. 2, April 2017, pp.67-72
e-ISSN 2519-9277, p-ISSN 2519-9269
Available online at http:// www.refaad.com

Binary Linear Codes and Binary Matrices

Driss Harzalla *1

University Chouaib Doukkali, Faculty of Sciences
Department of Mathematics, EI Jadida, Morocco
68harzalla@gmail.com

Abstract. In [1], the automorphism group of a binary linear code is computed by identifying it with one of its optimal generator matrices. This identification is effective for the computation of the automorphism group of a binary linear code. As application, we show in this work that the automorphism group of the binary triple-error-correcting primitive BCH code C of length $n = 31$ is the general linear group $GL_5(F_2)$ on the vector space F_{32} over F_2. Numerical examples are given by the use of some theoretical software : GAP 4.8.5 (Group Algorithm Programming), Q-extension and Grin 4.0 (Graph Interface).

Keywords: *Automorphism, Binary matrix, Bipartite graph, Optimal generator matrix, Binary BCH codes.*

1 Introduction

A linear $[n,k]-$code C over F_2 is a k-dimensional subspace of the vector space $(F_2)^n$. Let Cod_n be the set of all binary linear codes of dimension k and of fixed length n, the natural action of the symmetric group S_n on Cod_n is defined by: $\sigma(C) = \{\sigma((c_i)_i) = (c_{\sigma(i)})_i / c \in C\}$. We say that C_1 and C_2 are isomorphic or equivalent and we write $C_1 \cong C_2$ if and only if there exist $\sigma \in S_n$ such that $\sigma(C_1) = C_2$, σ is said to be an isomorphism and in case $C_1 = C_2$, σ is said to be an automorphism. We deduce from the above that for fixed n, $Aut(C) = \{\sigma \in S_n / \sigma(C) = C\}$ is the stabilizer $Stab_{S_n}(C)$ under the above natural action and $Aut(C)$ is then a subgroup of S_n called the automorphism group of C.
It is shown in [1] that a binary linear code and a binary matrix represent the same object in the sense that they have the same automorphism group up to an isomorphism. The determination of the structure of codes, computation of their weight distribution, classification of codes, decoding algorithm and cryptography, all these problems can be relatively simplified by the use of the notion of the automorphism group. In the general case the determination of automorphism group of linear codes and that of graphs is known to be a difficult problem.
A generator matrix G for a linear $[n,kbbb]-$code C is a $(k \times n)-$matrix whose rows form a basis for C, and its parity check matrix H is an $((n-k) \times n)-$matrix with property $GH^T = 0$ where 0 is the $k \times (n-k)$ null matrix.
Recall that the Hamming distance $d(m,m')$ between two code-words of a binary $[n,k]-$code C is the number of positions by which the two code-words differ. The Hamming weight $wt(m)$ of a code-word $m \in C$ is $d(m,0)$. A linear $[n,k,d]-$code C over F_2 is a k-dimensional subspace of the vector space $(F_2)^n$, where

$$d = d(C) = \min_{m \neq m' \in C} d(m,m') = \min_{0 \neq m \in C} wt(m).$$

Let $M_{k \times n}$ be the set of all $k \times n$ binary matrices with $k < n$ and let $A, B \in M_{k \times n}$. We define a natural action of S_n on $M_{k \times n}$ as follows: if $A = [c_1, c_2, ..., c_n]$ and $\sigma \in S_n$ then, $A\sigma = [c_{\sigma(1)}, c_{\sigma(2)}, ..., c_{\sigma(n)}]$. We say that A and B are isomorphic and we write $A \cong B$ if there exist $\sigma \in S_n$ such that the set $Rows(A\sigma)$ of rows of $A\sigma$ is equal to the set $Rows(B)$ of rows of B. σ is said to be an isomorphism and in case $A = B$, σ is said to be an automorphism. The set

$$Aut(A) = \{\sigma \in S_n / \ Rows(A\sigma) = Rows(A)\}$$

*Corresponding author.Driss Harzalla 68harzalla@gmail.com
2010 Mathematics Subject Classification: 94B05, 11T71.

is called the automorphism group of the binary matrix A which is a subgroup of S_n. We associate with the generator matrix G a binary matrix $B[G]$ as described in the following algorithm [1]:

The algorithm: we begin with the first row vector r_1 of G and we search all the code-words of C different from r_1 and having the same weight as r_1. If they exist they are all added at the beginning of G as row vectors, else we move to the second row vector r_2 of G and we repeat the same procedure as before. We repeat this process until exhaustion of all row vectors of G. This process ends and the binary matrix $B[G]$ is constructed (see [1, Theorem 2.1]).

Theorem: The code C and the binary matrix $B[G]$ have the same automorphism group: $Aut(C) = Aut(B[G])$

Corollary: If G_1 and G_2 are two generator matrices of the code C then the corresponding binary matrices $B[G_1]$ and $B[G_2]$ have the same automorphism group.

Definition: A generator matrix OG is said to be an *optimal* generator matrix of an $[n, k]-$code if we have $OG \in \underset{G \in Gen(C)}{\arg\min} \left(\sum_{i=1}^{i=k} A_{w_{g_i}} \right)$ where $Gen(C)$ is the set of all generator matrices G of the code C and $(A_{w_{g_i}})_{0 \leq i \leq n}$, $w_{g_i} = wt(g_i)$ the weight distribution of rows g_i of G. The associated binary matrix $OB[G]$ is also said to be optimal.

We recall that binary Bose-Chaudhuri-Hockenghem code or binary BCH code for short is the largest possible cyclic code of length n over the field F_2 , whose generator polynomial has zeros $a^b, a^{b+1}, a^{b+1}, ..., a^{b+\delta-2}$ where a is a primitive n^{th} root of unity in the splitting field F_{2^m}, b is an integer $0 \leq b \leq n - \delta + 1$ and m is the multiplicative order of 2 modulo n. The length n of the code and the size $q = 2$ of the field must be relatively prime. The generator polynomial is equal to the least common multiple of the minimal polynomials of $a^b, a^{b+1}, a^{b+1}, ..., a^{b+\delta-2}$. Special cases are $b = 1$ (resulting codes are called narrow-sense BCH codes), and $n = 2^m - 1$ (known as primitive BCH codes). The largest value of d for which the BCH code with designed distance d coincides with the BCH code with designed distance δ is called the Bose distance of the code. The true minimum distance of the code is greater than or equal to the Bose distance [3].

2 Application to binary BCH Code of parameters $n = 31$, $b = 1$, $\delta = 7$

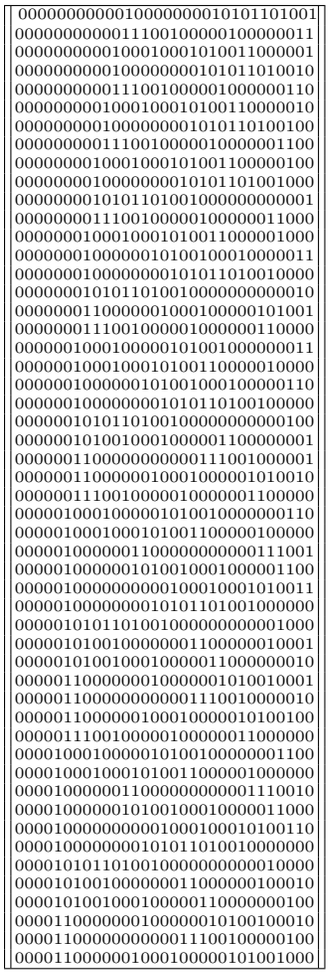
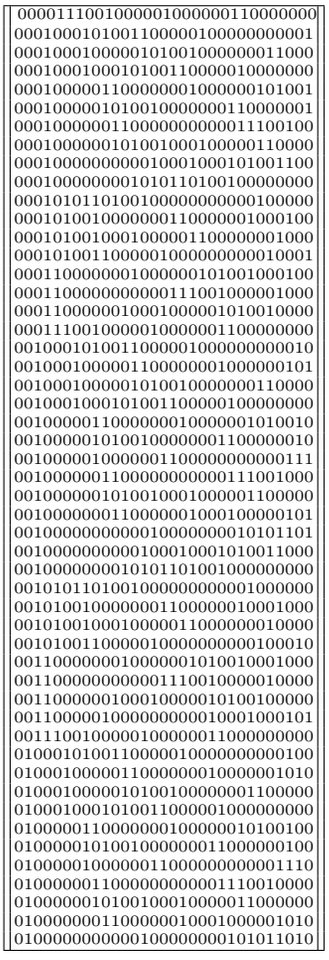
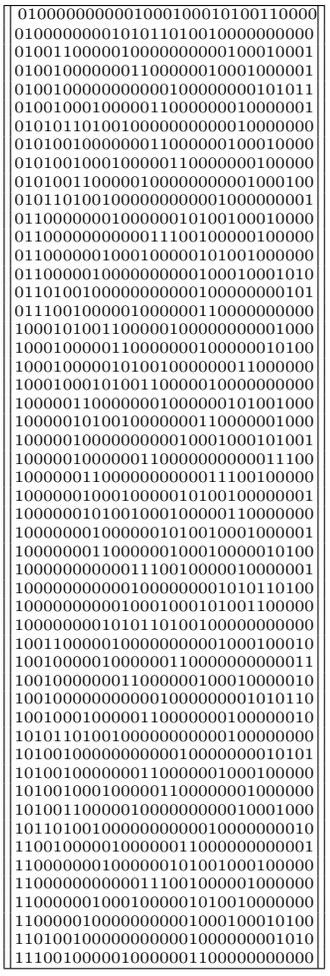
The weight distribution and the minimum distance of the binary narrow-sense primitive BCH code $C = BCHCode(n = 31, b = 1, \delta = 5, GF(2))$ of parameters $n = 31, b = 1, \delta = 5$ are given in the following GAP program

```
gap> C :=BCHCode( 31, 1, 5, GF(2) );
a cyclic [31, 21, 5]3 BCH code, delta= 5, b = 1 over GF(2)
gap> MinimumDistance(C);
7
gap> WeightDistribution(C);
[1, 0, 0, 0, 0, 0, 0, 0, 155, 465, 0, 0, 5208, 8680, 0, 0, 18259, 18259, 0, 0, 8680, 5208, 0, 0, 465,
155, 0, 0, 0, 0, 0, 0, 0, 1]
gap>
```

This code is a cyclic $[31, 16, 7]-$code of minimum distance 7, dimension 16, length 31 and its weight distribution is: $[1, 0, 0, 0, 0, 0, 0, 155, 465, 0, 0, 5208, 8680, 0, 0, 18259, 18259, 0, 0, 8680, 5208, 0, 0, 465, 155, 0, 0, 0, 0, 0, 1]$ By using the GAP command MinimumWeightWords(C), one can look for a generator matrix among the 155 words of minimal weight. And by using Q-Extension tools [2] the following optimal generator matrix is then obtained.

$$OG = \begin{pmatrix} 0000000000010000000010101101001 \\ 0000000000011100100000100000011 \\ 0000000001000100010100110000001 \\ 0000000001000000000101011010010 \\ 0000000000111001000001000000110 \\ 0000000001000100010100110000010 \\ 0000000001000000001010110100100 \\ 0000000010001000101001100000100 \\ 0000000100010001010011000001000 \\ 0000001000100000101001000000011 \\ 0000010001000001010010000000110 \\ 0000100010000010100100000001100 \\ 0001000101001100000100000000001 \\ 0010001010011000001000000000010 \\ 0100010100110000010000000000100 \\ 1000101001100000100000000001000 \end{pmatrix}$$

The optimal binary matrix associated with the code C is the binary $(155 \times 31)-$matrix of rows

By using Q-Extension tools [2], the set generating the group of the optimal binary matrix is obtained. Then, the GAP command GroupWithGenerators([ ]) determines the structure of this group as indicated in the next two programs.

- **Q-extension program:**

```
ok
?155 31 2
00000000000010000000010101101001
00000000000011100100000100000011
00000000001000100010100110000001
00000000001000000000101011010010
⋮  ⋮  ⋮
11000001000000000001000100010100
11010010000000000001000000001010
11100100000100000011000000000000
AUT: 9999360
(1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,)
Bed L 0 MAX L 6
Authomorphisms
aut-(5,8,)(10,25,)(11,23,)(14,22,)(15,26,)(16,17,)(18,27,)(29,31,)
aut-(5,10,)(8,25,)(11,17,)(14,29,)(15,27,)(16,23,)(18,26,)(22,31,)
aut-(5,11,)(8,23,)(10,17,)(14,15,)(16,25,)(18,31,)(22,26,)(27,29,)
aut-(5,14,)(8,22,)(10,29,)(11,15,)(16,18,)(17,27,)(23,26,)(25,31,)
aut-(4,5,)(7,31,)(8,21,)(9,23,)(11,30,)(13,29,)(18,28,)(24,27,)
aut-(3,4,)(6,30,)(7,20,)(8,22,)(10,29,)(12,28,)(17,27,)(23,26,)
aut-(2,3,)(6,19,)(7,21,)(8,31,)(9,28,)(10,14,)(15,17,)(18,23,)
aut-(1,2,)(6,20,)(7,30,)(9,13,)(10,26,)(11,31,)(15,25,)(23,29,)
```

- **GAP (GUAVA) program:**

```
gap> G :=GroupWithGenerators([(5,8)*(10,25)*(11,23)*(14,22)*(15,26)*(16,17)*(18,27)*(29,31),
(5,10)*(8,25)*(11,17)*(14,29)*(15,27)*(16,23)*(18,26)*(22,31),
(5,11)*(8,23)*(10,17)*(14,15)*(16,25)*(18,31)*(22,26)*(27,29),
(5,14)*(8,22)*(10,29)*(11,15)*(16,18)*(17,27)*(23,26)*(25,31),
(4,5)*(7,31)*(8,21)*(9,23)*(11,30)*(13,29)*(18,28)*(24,27),
(3,4)*(6,30)*(7,20)*(8,22)*(10,29)*(12,28)*(17,27)*(23,26),
(2,3)*(6,19)*(7,21)*(8,31)*(9,28)*(10,14)*(15,17)*(18,23),
(1,2)*(6,20)*(7,30)*(9,13)*(10,26)*(11,31)*(15,25)*(23,29)]);
<permutation group with 8 generators>
gap> StructureDescription(G);
"PSL(5,2)"
gap>
```

We deduce that the automorphism group of the the binary narrow-sense primitive BCH code $C = BCHCode(n = 31, b = 1, \delta = 5, GF(2))$ of parameters $n = 31, b = 1, \delta = 5$ is the special projective linear group $PSL(3, 2)$. We recall here that $PSL(5, 2) = SL(5, 2) = GL(5, 2)$, the special (general) linear group of 5×5 matrices over the field with 2 elements.

3 Conclusion

In general, let C be an $[n, k]-$code and OG its optimal generator matrix. Let r_i, $i = 1, 2, ..., k$ be the rows of OG and (A_{w_i}), $w_i = wt(r_i)$ its weight distribution.
Let OB be the optimal binary matrix described in the algorithm 1. Recall that $Aut(C)$ and $Aut(OB[G])$ are the same.
The method of the optimal binary matrix is effective since in the general case the value of

$$\frac{\min\limits_{G \in OGen(C)} \left(\sum\limits_{i=1}^{i=k} A_{w_i} \right)}{A_{w_1} + A_{w_2} + ... + A_{w_k}}$$

is very small.

In the example of the binary narrow-sense primitive BCH code $C = BCHCode(n = 31, b = 1, \delta = 5, GF(2))$ of parameters $n = 31, b = 1, \delta = 5$ we have:

$$\frac{\#Rows\left(OB\left[G\right]\right)}{\#Rows\left(\left[C\right]\right)} = \frac{155}{2^{16}} \approx 0,0023$$

The main result of this work is the result given in the following theorem.

Theorem 3.1. *The automorphism group of the binary triple-error-correcting primitive BCH code C of length $n = 2^m - 1 = 31$ with $m = 5$, is $GL_5(F_2)$, where $GL_5(F_2)$ is the general linear group on the vector space F_{32} over F_2.*

ACKNOWLEDGEMENTS.
The author gratefully acknowledge the referees for their useful suggestions and comments.

References

[1] D. Harzalla. *Optimal Generator matrix and the automorphism groups of linear binary codes*, International Journal of Engineering Issues, Infinity Science, 2:53–61, 2016.

[2] G. Iliya Bouyukliev. *What is Q-Extension?*, Serdica J. Computing, 1:553–564, 2007.

[3] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes*, Elsevier-North-Holland, Amsterdam, 1977.