Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 13, Number 9 (2017), pp. 5461-5468

http://www.ripublication.com

On [31, 28, 3] Hamming Code and [7, 4, 4] MDS Code Over GF(5)

Tarun Lata

Research Scholar,
Department of Mathematics, University of Delhi, Delhi -110007

Abstract

In this correspondence, we investigate Hamming codes for r = 3 over GF (5). We follow a simple construction procedure for the codes and also prove that the codes are perfect. MDS codes are also obtained by using the same construction technique under certain conditions. In particular, we study [31, 28, 3] 5-ary code and also show that it is a perfect code whereas [7, 4, 4] 5-ary code turns out to be MDS under certain conditions.

Keywords: Generator matrix, MDS code, Parity check matrix, Perfect code, Syndrome.

1. INTRODUCTION

A linear code V over GF(q) , where GF(q) is the Galois field, is a linear proper subspace of a vector space V^n which can be represented as the span of a minimal set of codewords known as basis. These basis are the rows of a matrix known as Generator matrix.
In this paper the weight of a vector v, denoted as w(v), is considered in Hamming sense as also the minimum distance between two non-zero codewords.
For correcting t errors, the minimum weight of a code should be (2t + 1) [4]. In other words, if d is the minimum distance of a code V, then V can correct t = $\left\lfloor \frac{d-1}{2} \right\rfloor$ or fewer errors. Such a code is denoted by [n, k, d] code of length n, rank k and minimum distance d.
For d = r +1 and for size of the code V = q^{n-r} is known as MDS code since it has maximum possible distance for given code size V and codeword length n [6].

According to Peterson and Weldon [4], every residue class modulo q contains either 0 or a positive integer less than q. Zero is an element of the ideal and each positive integer less than q is in a distinct residue class. It follows from the above theorem that the list {0}, {1}, {2}, . . . {q−1} includes each class once and only once. Another important theorem [4] gives the concept of prime fields or Galois field of q elements which we consider throughout this paper. According to the theorem, residue classes of integers modulo any positive prime integer q form a field of q elements known as Galois field GF(q). So, GF(5) comprises of 0,1,2,3 and 4 with the following addition and multiplication properties:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

This paper is organized into four sections. Section 2 gives construction procedure and error correcting capabilities are discussed in Section 3. Section 4 and 5 show that the codes are perfect and MDS respectively.

2. CONSTRUCTION

The number of distinct elements in the Cartesian product GF(5) × GF(5) × GF(5) is 125 in which 124 elements are non-zero. These non – zero elements can be partitioned into 31 disjoint sets in which any two pairs of the same set are multiple of each other over GF(5). The sets are as follows:

T_1 = (1,1,1),(2,2,2),(3,3,3),(4,4,4), T_2 = (1,1,2),(2,2,4),(3,3,1),(4,4,3), T_3 = (1,1,3),(2,2,1),(3,3,4),(4,4,2),
T_4 = (1,1,4),(2,2,3),(3,3,2),(4,4,1), T_5 = (1,2,1),(2,4,2),(3,1,3),(4,3,4), T_6 = (1,2,2),(2,4,4),(3,1,1),(4,3,3),
T_7 = (1,2,3),(2,4,1),(3,1,4),(4,3,2), T_8 = (1,2,4),(2,4,3),(3,1,2),(4,3,1), T_9 = (1,3,1),(2,1,2),(3,4,3),(4,2,4),
T_{10} = (1,3,2),(2,1,4),(3,4,1),(4,2,3), T_{11} = (1,3,3),(2,1,1),(3,4,4),(4,2,2), T_{12} = (1,3,4),(2,1,3),(3,4,2),(4,2,1),
T_{13} = (1,4,1),(2,3,2),(3,2,3),(4,1,4), T_{14} = (1,4.2),(2,3,4),(3,2,1),(4,1,3), T_{15} = (1,4,3),(2,3,2),(3,2,4),(4,1,2),
T_{16} = (1,4,4),(2,3,3),(3,2,2),(4,1,1), T_{17} = (1,1,0),(2,2,0),(3,3,0),(4,4,0), T_{18} = (1,2,0),(2,4,0),(3,1,0),(4,3,0),
T_{19} = (1,3,0),(2,1,0),(3,4,0),(4,2,0), T_{20} = (1,4,0),(2,3,0),(3,2,0),(4,1,0), T_{21} = (1,0,1),(2,0,2),(3,0,3),(4,0,4),
T_{22} = (1,0.2),(2,0,4),(3,0,1),(4,0,3), T_{23} = (1,0,3),(2,0,1),(3,0,4),(4,0,2), T_{24} = (1,0,4),(2,0,3),(3,0,2),(4,0,1),
T_{25} = (0,1,1),(0,2,2),(0,3,3),(0,4,4), T_{26} = (0,1,2),(0,2,4),(0,3,1),(0,4,3), T_{27} = (0,1,3),(0,2,1),(0,3,4),(0,4,2),
T_{28} = (0,1,4),(0,2,3),(0,3,2),(0,4,1), T_{29} = (1,0,0),(2,0,0),(3,0,0),(4,0,0), T_{30} = (0,1,0),(0,2,0),(0,3,0),(0,4,0),
T_{31} = (0,0,1),(0,0,2),(0,0,3),(0,0,4).

Now, we take 31 vectors, one from each set and use their transpose to construct the following 3×31 parity-check matrix H:

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 3 & 3 & 3 & 3 & 4 & 4 & 4 & 4 & 1 & 2 & 3 & 4 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 & 0 & 0 & 0 & 0 & 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 & 0 & 0 & 1 \end{bmatrix}.$$

Let $V = \{ x = (x_1,x_2,\text{----------},x_{31} \in GF(5)^{31} \mid Hx^T = 0 \};$

then, V is the subspace of $GF(5)^{31}$ and therefore a linear code over GF(5).

$Hx^T = 0$, which means

$$x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8 + x_9 + x_{10} + x_{11} + x_{12} + x_{13} + x_{14} + x_{15} + x_{16} + x_{17} + x_{18} + x_{19} + x_{20} + x_{21} + x_{22} + x_{23} + x_{24} + x_{29} = 0 \quad \text{----------(2.1)}$$

$$x_1 + x_2 + x_3 + x_4 + 2x_5 + 2x_6 + 2x_7 + 2x_8 + 3x_9 + 3x_{10} + 3x_{11} + 3x_{12} + 4x_{13} + 4x_{14} + 4x_{15} + 4x_{16} + x_{17} + 2x_{18} + 3x_{19} + 4x_{20} + x_{25} + x_{26} + x_{27} + x_{28} + x_{30} = 0 \quad \text{----------(2.2)}$$

$$x_1 + 2x_2 + 3x_3 + 4x_4 + x_5 + 2x_6 + 3x_7 + 4x_8 + x_9 + 2x_{10} + 3x_{11} + 4x_{12} + x_{13} + 2x_{14} + 3x_{15} + 4x_{16} + x_{21} + 2x_{22} + 3x_{23} + 4x_{24} + x_{25} + 2x_{26} + 3x_{27} + 4x_{28} + x_{31} = 0 \quad \text{----------(2.3)}$$

which then yields :

$$x_{29} = 4x_1 + 4x_2 + 4x_3 + 4x_4 + 4x_5 + 4x_6 + 4x_7 + 4x_8 + 4x_9 + 4x_{10} + 4x_{11} + 4x_{12} + 4x_{13} + 4x_{14} + 4x_{15} + 4x_{16} + 4x_{17} + 4x_{18} + 4x_{19} + 4x_{20} + 4x_{21} + 4x_{22} + 4x_{23} + 4x_{24} ,$$

$$x_{30} = 4x_1 + 4x_2 + 4x_3 + 4x_4 + 3x_5 + 3x_6 + 3x_7 + 3x_8 + 2x_9 + 2x_{10} + 2x_{11} + 2x_{12} + x_{13} + x_{14} + x_{15} + x_{16} + 4x_{17} + 3x_{18} + 2x_{19} + x_{20} + 4x_{25} + 4x_{26} + 4x_{27} + 4x_{28} ,$$

$$x_{31} = 4x_1 + 3x_2 + 2x_3 + x_4 + 4x_5 + 3x_6 + 2x_7 + x_8 + 4x_9 + 3x_{10} + 2x_{11} + x_{12} + 4x_{13} + 3x_{14} + 2x_{15} + x_{16} + 4x_{21} + 3x_{22} + 2x_{23} + x_{24} + 4x_{25} + 3x_{26} + 2x_{27} + x_{28} ,$$

Since x_1 , x_2 , x_3 , x_4 , x_5 ,-------, x_{26} ,x_{27} and x_{28} are independent variables and x_{29} , x_{30} and x_{31} are dependent variables, we can assign x_1 , x_2 , x_3 , x_4 , x_5 -----, x_{26} ,x_{27} and x_{28} conveniently chosen values. Thus setting x_1=1 and $x_2 = x_3 =$ ---------- $= x_{28} = 0$, we get $x_{29} = x_{30} = x_{31} = 4$. So, (1,0,0,0,-----,4,4,4) is a solution of (2.1), (2.2), and (2.3).
Similarly, we can find other 27 solutions (0,1,0,0,0,-----4,4,3),(0,0,1,0,0,-----, 4, 4, 2), ---------- and (0,0,0,0,0,-------,0,1,0,4,1).All these solutions are 28 codewords of V . Since they are independent, we can use these codewords to form 28×31 generator matrix G of V given by

G =
$$\begin{bmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&4&4&4\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&4&4&3\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&4&4&2\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&4&4&1\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&4&3&4\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&4&3&3\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&4&3&2\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&4&3&1\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&4&2&4\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&4&2&3\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&4&2&2\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&4&2&1\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&4&1&4\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&4&1&3\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&4&1&2\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&4&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&4&4&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&4&3&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&4&2&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&4&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&4&0&4\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&4&0&3\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&4&0&2\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&4&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&4&4\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&4&3\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&4&2\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&4&1
\end{bmatrix}$$

This completes the construction of the [31, 28, 3] code over GF(5). Let us now discuss its error correcting capabilities.

3. MINIMUM WEIGHT OF THE CODE

Theorem 3.1 : The minimum weight of the Hamming code over GF(5) is 3.

Proof: We see that the weight of each row in G is at least 3.

Now, let $\alpha , \beta \neq 0 , i \neq j , 1 \leq i , j \leq 28$.

Then, $\alpha(28,i) + \beta(28,j) = (28\alpha, \alpha i) + (28\beta, \beta j) = (28(\alpha + \beta), \alpha i + \beta j)$.

Two cases may arise here:

Case 1: $\alpha+\beta = 0$.

Then, $\beta = - \alpha$ and $\alpha i+\beta j = \alpha i – \alpha j = \alpha(i – j) \neq 0$ as $i \neq j$.

Case 2: $\alpha + \beta \neq 0$.

Then, $28(\alpha + \beta) \neq 0$

Hence $\alpha , \beta \neq 0 , i \neq j , 1 \leq i , j \leq 28$,

$\alpha(28,i) + \beta(28,j) \neq (0,0)$.

So, a linear combination of any two rows of G with non-zero scalars from GF(5) has weight at least 3.

A linear combination of any number of rows of G has weight at least 3.

Hence, the minimum weight of V is 3.

Corollary 3.1: The [31, 28, 3] Hamming code over GF(5) corrects 1 error.

Proof: As we know that if d is the minimum weight of a code, then V can correct $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ or fewer errors.

Since, d of V is 3, then t = 1.
Hence, V can correct only 1 error.
Thus, the [31, 28, 3] code is a single error correcting code.

4. PERFECT CODE

An [n, k] linear code V of minimum weight d = 2t + 1 over GF(q) is known as perfect if it will correct all error -patterns of weight less than or equal to t and no other error patterns.
So, [31, 28, 3] 5-ary Hamming code is said to be perfect if it corrects all error pattern of weight 1 and no other error patterns. It can be easily verified by error-pattern and syndrome table that [31, 28] 5-ary code is a single error correcting perfect code.

Error-Pattern and Syndrome Table

Error-Pattern	Syndrome	Error-Pattern	Syndrome
1000000000000000000000000000000	111	3000000000000000000000000000000	333
0100000000000000000000000000000	112	0300000000000000000000000000000	331
0010000000000000000000000000000	113	0030000000000000000000000000000	334
0001000000000000000000000000000	114	0003000000000000000000000000000	332
0000100000000000000000000000000	121	0000300000000000000000000000000	313
0000010000000000000000000000000	122	0000030000000000000000000000000	311
0000001000000000000000000000000	123	0000003000000000000000000000000	314
0000000100000000000000000000000	124	0000000300000000000000000000000	312
0000000010000000000000000000000	131	0000000030000000000000000000000	343
0000000001000000000000000000000	132	0000000003000000000000000000000	341
0000000000100000000000000000000	133	0000000000300000000000000000000	344
0000000000010000000000000000000	134	0000000000030000000000000000000	342
0000000000001000000000000000000	141	0000000000003000000000000000000	323
0000000000000100000000000000000	142	0000000000000300000000000000000	321
0000000000000010000000000000000	143	0000000000000030000000000000000	324
0000000000000001000000000000000	144	0000000000000003000000000000000	322
0000000000000000100000000000000	110	0000000000000000300000000000000	330
0000000000000000010000000000000	120	0000000000000000030000000000000	310
0000000000000000001000000000000	130	0000000000000000003000000000000	340
0000000000000000000100000000000	140	0000000000000000000300000000000	320
0000000000000000000010000000000	101	0000000000000000000030000000000	303
0000000000000000000001000000000	102	0000000000000000000003000000000	301
0000000000000000000000100000000	103	0000000000000000000000300000000	304
0000000000000000000000010000000	104	0000000000000000000000030000000	302
0000000000000000000000001000000	011	0000000000000000000000003000000	033
0000000000000000000000000100000	012	0000000000000000000000000300000	031
0000000000000000000000000010000	013	0000000000000000000000000030000	034
0000000000000000000000000001000	014	0000000000000000000000000003000	032
0000000000000000000000000000100	100	0000000000000000000000000000300	300
0000000000000000000000000000010	010	0000000000000000000000000000030	030
0000000000000000000000000000001	001	0000000000000000000000000000003	003
2000000000000000000000000000000	222	4000000000000000000000000000000	444
0200000000000000000000000000000	224	0400000000000000000000000000000	443

00200000000000000000000000000000	221	00400000000000000000000000000000	442
00020000000000000000000000000000	223	00040000000000000000000000000000	441
00002000000000000000000000000000	242	00004000000000000000000000000000	434
00000200000000000000000000000000	244	00000400000000000000000000000000	433
00000020000000000000000000000000	241	00000040000000000000000000000000	432
00000002000000000000000000000000	243	00000004000000000000000000000000	431
00000000200000000000000000000000	212	00000000400000000000000000000000	424
00000000020000000000000000000000	214	00000000040000000000000000000000	423
00000000002000000000000000000000	211	00000000004000000000000000000000	422
00000000000200000000000000000000	213	00000000000400000000000000000000	421
00000000000020000000000000000000	232	00000000000040000000000000000000	414
00000000000002000000000000000000	234	00000000000004000000000000000000	413
00000000000000200000000000000000	231	00000000000000400000000000000000	412
00000000000000020000000000000000	233	00000000000000040000000000000000	411
00000000000000002000000000000000	220	00000000000000004000000000000000	440
00000000000000000200000000000000	240	00000000000000000400000000000000	430
00000000000000000020000000000000	210	00000000000000000040000000000000	420
00000000000000000002000000000000	230	00000000000000000004000000000000	410
00000000000000000000200000000000	202	00000000000000000000400000000000	404
00000000000000000000020000000000	204	00000000000000000000040000000000	403
00000000000000000000002000000000	201	00000000000000000000004000000000	402
00000000000000000000000200000000	203	00000000000000000000000400000000	401
00000000000000000000000020000000	022	00000000000000000000000040000000	044
00000000000000000000000002000000	024	00000000000000000000000004000000	043
00000000000000000000000000200000	021	00000000000000000000000000400000	042
00000000000000000000000000020000	023	00000000000000000000000000040000	041
00000000000000000000000000002000	200	00000000000000000000000000004000	400
00000000000000000000000000000200	020	00000000000000000000000000000400	040
00000000000000000000000000000020	002	00000000000000000000000000000040	004
00000000000000000000000000000002		00000000000000000000000000000004	

5. MDS CODE

An [n, k, d] linear code is said to be MDS code if it satisfies the Singleton bound which states that $d = n – k +1$[7].

In order to show that [7, 4] 5-ary code is a MDS code, we have to show that the minimum weight of the code is 4.

We know that the number of codewords in a q-ary code is always the power of q. If the rank of the parity check matrix H is $r = n- k$, then the number of codewords is q^{n-k}. Singleton [7] has proved a theorem and discussed its corollaries that relate distance with the columns of the parity check matrix H as given below.

Theorem 5.1: A linear q-ary code with parity check matrix H has (minimum) q-ary distance d if and only if

(i) Every subset of d -1 columns of H is linearly independent.

(ii) Subset of d columns of H is linearly dependent.

Corollary 5.1: For a linear q-ary code, d = r+1 if and only if every set of r columns of its parity check matrix H is linearly independent.

Corollary 5.2: If the parity check matrix of a linear q-ary code is of the form H= [A ⋮ I], then d = r + 1 if and only if every square submatrix of order j within A where $1 \leq j \leq \min(r ; k)$ has a non-zero determinant.

DISCUSSION

If we take 4 pairs (in which at least two elements of these pairs are distinct) from T_1 to T_{31} whose all three elements are non-zero and taking their transpose. Then we can make parity –check matrix H_1 along with identity matrix of order 3 for MDS code.

$$H_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 2 & 3 & 4 & 0 & 1 & 0 \\ 2 & 3 & 4 & 1 & 0 & 0 & 1 \end{bmatrix}$$

H_1 can be written as $H_1 = [A : I]$, Where,

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix} \quad \text{and} \quad I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Every pair of two columns of H is linearly independent and every column of A can be formed by the linear combination of columns of I.

Since every square sub-matrix of order 1, 2 and 3 within A has a non-zero determinant, so, by Theorem 5.1, the minimum distance d of H_1 is 4 and d = n- k + 1.

So, the [7, 4, 4] code is a MDS code over GF(5).

ACKNOWLEDGEMENT

The author would like to thank Dr. Vinod Tyagi, University of Delhi for his guidance in pursuing research.

REFERENCES

[1] F.K. Elora, A.K.M.T. Rian and P.P. Dey, 2014. On quinary hamming code for r = 2, International Journal of Computer and Information Technology. 5 1069-1073.

[2] R. Hill, 1986. A First Course in Coding Theory, The Oxford University Press.

[3] W.C. Huffman and V. Pless, 2003. Fundamentals of Error Correcting Codes, Cambridge University Press, New York.

[4] T. Lata and V. Tyagi, 2015. New Construction Technique for q-ary Hamming

codes for r =2, q ≥ 3, International Journal of Applied Mathematics. 28 799-806.

[5] W.W. Peterson and E.J. Weldon, 1972. Error-correcting Codes. 2nd Ed., MIT Press.

[6] V. Pless, 2003. Introduction to the Theory of Error Correcting Codes. Wiley Student Ed., John Wiley & Sons (Asia), Singapore.

[7] R.C. Singleton, 1964. Maximum distance q-nary codes, IEEE Transactions on Information. 116–118.