NEW CONSTRUCTION TECHNIQUE FOR
q-ARY HAMMING CODES FOR r = 2, q ≥ 3

Tarun Lata¹ §, Vinod Tyagi²
¹Department of Mathematics
University of Delhi
Delhi, 110007, INDIA
²Department of Mathematics
Shyamlal College (Evening)
University of Delhi
Delhi, 110032, INDIA

Abstract: In this paper, we explore a new construction technique for q-ary Hamming codes \([q + 1, q - 1, 3]\) for \(r = 2\) and \(q ≥ 3\) over GF(q).

We also establish its perfectness and investigate its duality by using the MDS property.

AMS Subject Classification: 11T71, 94B05, 94D35, 94B60
Key Words: linear code, generator matrix, parity-check matrix, perfect code, MDS code

1. Introduction

As binary codes are based on two symbols 0 and 1 and a q-ary code is based on q-symbols 0, 1, 2, . . . , q − 1. For \(d = r + 1\) and size of the code \(N = q^k\). These codes are called MDS codes since they have maximum possible distance for given code size \(N\) and codeword length \(n\) [6].

According to Peterson et al. [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 \( \{0\}, \{1\}, \{2\}, \ldots \{q-1\} \) 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 \( q \) from a field of \( q \) elements known as Galois field \( \text{GF}(q) \).

A linear code of length \( n \), rank \( k \) and minimum weight \( d \) is called \([n, k, d]\) code. If \( V \) is a linear code with minimum distance \( d \), then \( V \) can correct \( t = \left\lfloor \frac{d-1}{2} \right\rfloor \) or fewer errors and conversely.

In this paper we consider only non-binary codes over \( \text{GF}(q) \), \( q \geq 3 \). It is organized as follows: We give detailed description of the construction of a \([q+1, q-1]\) linear code, \( V \) in Section 2. We show that the code \( V \) and its dual \( V^\perp \) are MDS code in Section 3. In Section 4, we prove that \([q+1, q-1, 3]\) linear code is a perfect code, whereas in Section 5, we give the decoding procedure. This is followed by an example for \( q = 3 \) in Section 6. Open problems are given in Section 7.

2. Construction

As we know, \( \text{GF}(q) \) is a Galois field of order \( q \), \( q \geq 3 \). The Cartesian product \( \text{GF}(q) \times \text{GF}(q) \) comprises the distinct \( q^2 \) pairs, i.e.

\[ |\text{GF}(q) \times \text{GF}(q)| = q^2. \]

The number of non-zero elements of \( \text{GF}(q) \times \text{GF}(q) = q^2 - 1 \). We can split the \((q^2 - 1)\) non-zero elements into \((q + 1)\) disjoint sets:

\[
S_1 = (1, 1), (2, 2), \ldots, (q - 1, q - 1),
S_2 = (1, 2), (2, 4), \ldots, (q - 1, 2(q - 1)),
\vdots
S_{q-2} = (1, q - 2), (2, 2q - 4), \ldots, (q - 1, (q - 2)(q - 1)),
S_{q-1} = (1, q - 1), (2, 2q - 2), \ldots, (q - 1, (q - 1)^2),
S_q = (1, 0), (2, 0), \ldots, (q - 1, 0),
S_{q+1} = (0, 1), (0, 2), \ldots, (0, q - 1),
\]

where any two pairs of the same set are multiples of each other over \( \text{GF}(q) \).

For the construction of parity check matrix, we take \((q + 1)\) pairs one from each set namely \((1, 1), (1, 2), \ldots, (1, 0), (0, 1)\) from \( S_1, S_2, \ldots, S_{q+1} \) respectively
and use their transposes to form the following $2 \times (q + 1)$ parity check matrix $H$:

$$H = \begin{bmatrix} 1 & 1 & \cdots & 1 & 1 & 0 \\ 1 & 2 & \cdots & q - 1 & 0 & 1 \end{bmatrix} \quad (2.1)$$

or

$$H = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 3 & \cdots & q - 1 & I_2 \end{bmatrix}.$$

Let $V = \{ x = (x_1, x_2, \ldots, x_{q+1}) \in \text{GF}(q)^{q+1} \mid Hx^T = 0 \}$. Then $V$ is a subspace of $\text{GF}(q)^{q+1}$ and therefore a linear code over $\text{GF}(q)$. Further, $Hx^T = 0$ implies that

\[
\begin{align*}
\begin{cases}
   x_1 + x_2 + \ldots + x_{q-1} + x_q = 0 \\
   x_1 + 2x_2 + \ldots + (q - 1)x_{q-1} + x_{q+1} = 0
\end{cases}
\end{align*}
\]

which then yields:

\[
\begin{align*}
x_q &= (q - 1)x_1 + (q - 1)x_2 + \ldots + (q - 1)x_{q-1}, \\
x_{q+1} &= (q - 1)x_1 + (q - 2)x_2 + \ldots + 2x_{q-2} + x_{q-1},
\end{align*}
\]

since $x_1, x_2, \ldots, x_{q-1}$ are independent variables and $x_q$ and $x_{q+1}$ are dependent variables.

We can assign to $x_1, x_2, \ldots, x_{q-1}$ conveniently chosen values. Thus we set $x_1 = 1$ and $x_2 = x_3 = \ldots = x_{q-1} = 0$ and get $x_q = q - 1$ and $x_{q+1} = q - 1$.

Thus, $(1, 0, 0, \ldots, 0, q - 1, q - 1)$ is a solution of (2.2). Similarly, $(0, 1, \ldots, 0, q - 1, q - 2), (0, 0, 1, \ldots, 0, q - 1, q - 3) \ldots$ and $(0, 0, 0, \ldots, 1, q - 1, 1)$ are $(q - 1)$ codewords of $V$. Since they are independent, we can use these codewords to form a $(q - 1) \times (q + 1)$ generator matrix $G$ of $V$ given by

\[
G = \begin{bmatrix} 1 & 0 & \cdots & 0 & q - 1 & q - 1 \\ 0 & 1 & \cdots & 0 & q - 1 & q - 2 \\ 0 & 0 & \cdots & 0 & q - 1 & q - 3 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & q - 1 & 1 \end{bmatrix}
\]

or

\[
G = \begin{bmatrix} q - 1 & q - 1 \\ q - 1 & q - 2 \\ q - 1 & q - 3 \\ \vdots & \vdots \\ q - 1 & 1 \end{bmatrix}.
\]
By this way, we have shown the construction of the \([q + 1, q - 1, d] \) code for all values of \(q \geq 3\).

3. MDS Code

In order to show that \([q + 1, q - 1, d] \) code is a MDS code, we have to show that the minimum weight of the code is 3. As 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 [6] has proved the following theorem that relates distance with the columns of the check matrix \(H\).

**Theorem 3.1.** 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 3.1.** 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 3.2.** 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**

We can write the parity check matrix \(H\) in equation (2.1) as

\[
H = \begin{bmatrix}
1 & 1 & 1 & \cdots & 1 & 1 & 0 \\
1 & 2 & 3 & \cdots & q-1 & 0 & 1
\end{bmatrix}.
\]

We can write \(H\) as

\[
H = [ A \ I ],
\]

where \(A = \begin{bmatrix}
1 & 1 & 1 & \cdots & 1 \\
1 & 2 & 3 & \cdots & q-1
\end{bmatrix}\) and \(I = \begin{bmatrix}
1 & 0 \\
0 & 1
\end{bmatrix}\).

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 submatrix of order 1 and 2 within $A$ has a non-zero determinant. So, by Theorem 3.1, Corollary 3.1 and Corollary 3.2, the minimum distance $d$ of $H$ is 3 and $d = n - k + 1$.

Hence the linear code $V$ is a MDS code. We also know that dual of a MDS code is also MDS. So, the dual of $V$, denoted by $V^\perp$, is also a MDS code.

The minimum weight of the $[q + 1, q - 1]$ Hamming code $V$ over GF$(q)$ is 3. So, is a single error correcting code.

It follows from the fact that if $d$ is the minimum weight of a code $V$. Then $V$ can correct $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ or fewer errors.

Since the minimum distance $d$ of $V$ is 3. Then $t = \left\lfloor \frac{3-1}{2} \right\rfloor = 1$.

Let $V^\perp = \{ u \in GF(q)^{q+1} | u \cdot v = 0 \ \forall \ v \in V \}$.

Then $V^\perp$ is the dual code of $V$. We know that dual of MDS code is also MDS code. So, $V^\perp$ is a $[q+1, 2]$ code with minimum distance $q+1-2+1 = q$.

Thus, $V^\perp$ can correct $\frac{q-1}{2}$ errors.

So, we have shown that the $[q + 1, q - 1, 3]$ code, $V$ and its dual are MDS codes over GF$(q)$ for all values of $q \geq 3$.

### 4. Perfect Code

An $[n, k]$ linear code $V$ of minimum weight $d = 2t + 1$ over GF$(q)$ is said to be perfect if the code $V$ will correct all error patterns of weight less than or equal to $t$ and no other error patterns.

Thus, we can say that a $[q + 1, q - 1, 3]$ $q$-ary Hamming code is said to be perfect if it corrects all error pattern of weight 1 and no other error patterns.

Now, we take distinct non-zero $(q + 1)$-tuple (error patterns) in which only one element is non-zero and others are zero, for all $1 \leq i \leq q - 1$ and find distinct $(q + 1)$ syndrome for each $1 \leq i \leq q - 1$.

<table>
<thead>
<tr>
<th>Error-Pattern</th>
<th>Syndrome</th>
</tr>
</thead>
<tbody>
<tr>
<td>$i \ (1,0,0,\ldots,0,0,0,0)$</td>
<td>$i \ (1 \ 1)$</td>
</tr>
<tr>
<td>$i \ (0,1,0,\ldots,0,0,0,0)$</td>
<td>$i \ (1 \ 2)$</td>
</tr>
<tr>
<td>$\vdots$</td>
<td>$\vdots$</td>
</tr>
<tr>
<td>$i \ (0,0,0,\ldots,0,1,0,0)$</td>
<td>$i \ (1 \ q-1)$</td>
</tr>
<tr>
<td>$i \ (0,0,0,\ldots,0,0,1,0)$</td>
<td>$i \ (1 \ 0)$</td>
</tr>
<tr>
<td>$i \ (0,0,0,\ldots,0,0,0,1)$</td>
<td>$i \ (0 \ 1)$</td>
</tr>
</tbody>
</table>
Here, total number of distinct non-zero error-patterns = 
\[(q - 1)(q + 1) = q^2 - 1.\]
Hence, by the condition given above, code \( V \) is a perfect code.

5. Decoding Algorithm

We conclude this paper by presenting decoding procedure for \( q \)-ary \([q+1, q-1, 3]\)
code in the following steps:

**Step 1:** Form \( H \).

**Step 2:** Compute \( Hr^T \), where \( r \) is the received vector.

(a) If \( Hr^T = \alpha \cdot j^{th} \) column of \( H \), where \( j \in \{1, 2, \ldots, q - 1\} \) and \( \alpha \in \text{GF}(q) \) such that \( \alpha \neq 0 \), the error has occurred in the the \( j^{th} \) co-ordinate of the sent code word, \( v \) and the error vector, \( e \) has field element \( \alpha \) in its \( j^{th} \) co-ordinate and zeros in other co-
ordinates.
So, \( e = (0, 0, \ldots, \alpha, \ldots, 0, 0) \), where \( \alpha \) is the \( j^{th} \) co-ordinate of \( e \).

(b) If \( Hr^T = 0 \), then there is no error,
i.e. \( r \) is a codeword of \( V \).

Suppose we want to send the code vector \( v = (1, 1, 1, \ldots, 1, 0) \) which is received
at the receiving end as \( r = (1, 1, 3, 1, \ldots, 1, 0) \). Then error vector, \( e = r - v = (0, 0, 2, 0, \ldots, 0) \). Now, to recover the code vector \( v \) from \( r \).

We compute \( Hr^T \) as follows:

\[
Hr^T = H(v + e)^T.
\]
Since \( v \in \text{ker} \, H \), then \( Hv^T = [0 \quad 0] \).

\[
Hr^T = [0 \quad 0] + 2 [1 \quad 3] = 2 [1 \quad 3]
\]
\[
= 2 \cdot 3^{rd} \text{ column of } H.
\]
This shows that error vector \( e \) contains the field element 2 in the 3\(^{rd}\) co-ordinate and error has occurred in the 3\(^{rd}\) co-ordinate of the code vector \( v \). Since \( e = r - v \), we obtain \( v \) from \( r - e \).

\[
v = r - e = (1, 1, 3, 1, 1, \ldots, 1, 0) - (0, 0, 2, 0, 0, \ldots, 0).
\]
\[
\Rightarrow v = (1, 1, 1, 1, \ldots, 1, 0).
\]
6. Conclusion

In this section, we discuss our work with the help of an illustration for \( q = 3 \) which follows as:

GF(3) comprises 0, 1 and 2.

\(|\text{GF}(3) \times \text{GF}(3)| = 9\). The number of non-zero elements of \(\text{GF}(3) \times \text{GF}(3)\) = 9 - 1 = 8.

We can split the 8 non-zero elements into 4 disjoint sets:

\( S_1 = (1, 1), (2, 2) \), \( S_2 = (1, 2), (2, 1) \), \( S_3 = (1, 0), (2, 0) \), \( S_4 = (0, 1), (0, 2) \).

Now, we form parity-check matrix by taking 4 pairs, one from each set, namely (1,1), (1,2), (1,0), (0,1) from \( S_1, S_2, S_3, S_4 \), respectively and use their transpose to form the following 2 × 4 parity-check matrix \( H_1 \):

\[
H_1 = \begin{bmatrix}
1 & 1 & 1 & 0 \\
1 & 2 & 0 & 1
\end{bmatrix}.
\]

Let \( V_1 = \{ x = (x_1, x_2, x_3, x_4) \in \text{GF}(3)^4 \mid H_1 x^T = 0 \} \).

\( H_1 x^T = 0 \) implies that

\[
\begin{align*}
x_1 + x_2 + x_3 &= 0 \\
x_1 + 2x_2 + x_4 &= 0
\end{align*}
\]

which then yields

\[
\begin{align*}
x_3 &= 2x_1 + 2x_2, \\
x_4 &= 2x_1 + x_2.
\end{align*}
\]

Here, \( x_1 \) and \( x_2 \) are independent variables and \( x_3, x_4 \) are dependent variables.

Setting \( x_1 = 1 \) and \( x_2 = 0 \), we get (1,0,2,2) is a solution of (6.1) and by setting \( x_1 = 0 \) and \( x_2 = 1 \), we get (0,1,2,1) as another solution of (6.1).

(1,0,2,2) and (0,1,2,1) are 2 codewords of \( V_1 \) and form its generator matrix \( G_1 \):

\[
G_1 = \begin{bmatrix}
1 & 0 & 2 & 2 \\
0 & 1 & 2 & 1
\end{bmatrix}.
\]

\( V_1, [4,2,3] \) code is a MDS code and corrects 1 error.

\( V_1^\perp, [4,2,3] \) code is also a MDS code which can correct 1 error.

Now we discuss the perfectness of \( V_1 \) by Error-Pattern Syndrome table:
The total non-zero distinct error pattern $= 8 = 3^2 - 1$. Hence, $V_1$ is a perfect code over GF(3).

Elora et al. [1] have already proved the perfectness of code for $q = 5$ by another method. We have also verified the above results for $q = 7, 11, 13$.

7. Open Problem

In this paper we have shown a general construction method of $q$-ary Hamming codes for prime field/Galois field. We have not been able to justify the result for the field of polynomials over GF($q$) modulo an irreducible polynomial of degree $m$ which is known as the Galois field of $q^m$ elements of GF($q^m$).

References


