Optimal Linear Codes Over $GF(7)$ and $GF(11)$ with Dimension 3

M. Emami*, L. Pedram

Department of Mathematics, University of Zanjan, Zanjan, I. R. Iran.

E-mail: emami@znu.ac.ir
E-mail: leilapedram@yahoo.com

Abstract. Let $n_q(k, d)$ denote the smallest value of $n$ for which there exists a linear $[n, k, d]$-code over the Galois field $GF(q)$. An $[n, k, d]$-code whose length is equal to $n_q(k, d)$ is called optimal. In this paper we present some matrix generators for the family of optimal $[n, 3, d]$ codes over $GF(7)$ and $GF(11)$. Most of our given codes in $GF(7)$ are non-isomorphic with the codes presented before. Our given codes in $GF(11)$ are all new.

Keywords: Linear codes, Optimal codes, Griesmer bound.

2010 Mathematics Subject Classification: 68P30, 94A29.

1. Introduction

Let $V_n(q)$ be the vector space of all ordered $n$-tuples over $GF(q)$ (Galois field of $q$ elements). Each subspace of $V_n(q)$ is called a linear code. By an $[n, k, d]$-code of length $n$ and dimension $k$ over $GF(q)$ we mean a $k$-dimensional subspace of $V_n(q)$ with minimum Hamming distance $d$. Sometimes we use the term $[n, k]$-code if the minimum distance $d$ is not under consideration. Optimizing any one of the parameters $n, k$ and $d$, when the other two values are given is one of the main problems in coding theory. These problems over a

*Corresponding Author

Received 31 January 2013; Accepted 13 September 2014
©2015 Academic Center for Education, Culture and Research TMU
fixed $GF(q)$ can be characterized as follows [7,9,11]:

1. What is the maximum value of $d$ (denoted by $d_q(n,k)$) for which there exists an $[n,k,d]$-code?
2. What is the minimum value of $n$ (denoted by $n_q(k,d)$) for which there exists an $[n,k,d]$-code?
3. What is the maximum value of $k$ (denoted by $k_q(n,d)$) for which there exists an $[n,k,d]$-code?

For a literature backlog of this topic when $q = 2, 3, 5$ and $7$ one is referred to [2,3,4,5,7,9,14,15,17,18,21,22,23]. In this paper we consider the problem for the case of codes over $GF(7)$ and $GF(11)$. In section 2 we give a brief review of our method. In Section 3 we give some basic necessary preliminaries. In Section 4 and 5 we study the value of functions $n_7(k,d)$ and $n_{11}(k,d)$ for $k \leq 3$ and some values of $d$.

2. A Brief Review of Our Method

In all parts of this study we followed a random process to obtain generator matrices for specified codes. For a given $k$ and $d$, the length $n$ of the optimal code can be obtained from the Griesmer bound and the existence of a possible $[n,k,d]$-code can be investigated by the MacWilliams identities. In case of nonexistence, we try to produce an $[n+1,k,d]$-code. In case of existence, the weight distributions given by MacWilliams identities help us to produce the code. We generate matrices of size $k \times n$ by a random process (based on a computer programming), we then test each of these matrices to be a generator matrix for a specific $[n,k,d]$-code. Since the parameters are small, in case of necessity we may produce all code words to find the weight distributions of the code to see whether the weight distributions satisfy the MacWilliams identities.

In quasi-cyclic codes we studied only the cases where $n$ is a multiple of $k$. Now since $n = ks$, for some positive integer “$s$”, we produced the first row of each of the $s$ circulant matrices $G_i$ of size $k \times k$, by the same random process, where $G = [G_1|G_2|\cdots|G_s]$ by the notations given in the corresponding section, is the generating matrix of a code. The remaining rows of each $G_i$ would fill cyclically. In last step the weight distributions should be tested.

As an example the $QC[32,4,25]$-code is consist of 8 circulant matrices of size $4 \times 4$, which is built as above. Gulliver method, as cited in Grassl code table [6], gives a different construction for this code which is based on two polynomials of degree 15 to produce the first rows of two matrices of sizes $4 \times 16$.

Also, it is important to note that in [4] as cited in Grassl table [6], the study uses the following method: given the parameters $n$ and $k$, the optimality of code is focused on $d$ (minimum distance), whereas in our papers, we employ a
different method: given the parameters k and d, the optimality is focused on n. Sure both methods reach to a unique optimal code, while the methods are completely different. In quasi cyclic codes we tried to find the generating matrices, where their weight distributions satisfy MacWilliams identities, meanwhile the other references such as [4] have a different approach.

For more emphasis on the originality of our methods and our results we tested some of our generator matrices, for any possible isomorphism, compared with the generator matrices given in Grassl table [6]. So we computed the weight distributions of some of the codes given in Grassl tables by a computer programming and found that they are all completely different.

For example our QC[20,4,15] and [32,4,25]-codes are both non-isomorphic with the same QC[20,4,15] and [32,4,25] codes given in Grassl table, as their weight distributions are different. One of the [28,4,21]-codes and two of the [24,4,18]-codes given in Grassl table, are all non-isomorphic from our corresponding codes (their weight distributions are different).

3. Preliminaries

let \( w(x) \) denotes the Hamming weight of a vector \( x \). That is the number of nonzero entries in \( x \). For a linear code, the minimum distance \( d \) is equal to the smallest value of \( w(x) \) when \( x \) range over all nonzero codewords. Let \( C \) be an \([n,k]\)-code and let \( A_i \) and \( B_i \) be the number of codewords of weight \( i \) in \( C \) and in dual code \( C^\perp \), respectively [9]. Now note that:

**Theorem 3.1.** (The MacWilliams identities [19]). Let \( C \) be an \([n,k]\)-code over \( GF(q) \). Then the \( A_i \)'s and \( B_i \)'s satisfy

\[
\sum_{j=0}^{n-t} \binom{n-j}{t} A_j = q^{k-t} \sum_{j=0}^{t} \binom{n-j}{n-t} B_j, \tag{3.1}
\]

for \( t = 0, 1, \ldots, n \).

**Lemma 3.2.** [9]. For an \([n,k,d]\)-code over \( GF(q) \), \( B_i = 0 \) for each value of \( i \) (where \( 1 \leq i \leq k \)) such that there does not exist an \([n-i,k-i+1,d]\)-code.

**Lemma 3.3.** [10] : Let \( C \) be an \([n,k,d]\)-code over \( GF(q) \) with \( k \geq 2 \), and with weight enumerator \( \sum_{i=0}^{n} A_i z^i \). Then

(i) if \( x \) and \( y \) are a linearly independent pair of codeword of \( C \),

\[
w(x) + w(y) \leq qn - qd + d, \tag{3.2}
\]

(ii) \( A_i = 0 \) for \( i > q(n-d) \).

**Corollary 3.4.** (I) Let \( C \) be an \([n,k,d]\)-code over \( GF(7) \) with \( k \geq 2 \). Then :

(i) if \( x \) and \( y \) are a linearly independent pair of codewords of \( C \), then \( w(x) + w(y) \leq 7n - 6d \),

(ii) \( A_i = 0 \) for \( i > 7(n-d) \),
(iii) \( A_i = 0 \) or 6 for \( i > 1/2(7n - 6d) \),
(iv) if \( A_i > 0 \), then \( A_j = 0 \) for \( j > 7n - 6d - i \) and \( i \neq j \);

(II) If \( C \) be an \([n, k, d]\)-code over \( GF(11) \) with \( k \geq 2 \), then :

(i) if \( x \) and \( y \) are a linearly independent pair of codewords of \( C \), then \( w(x) + w(y) \leq 11n - 10d \),
(ii) \( A_i = 0 \) for \( i > 11(n - d) \),
(iii) \( A_i = 0 \) or 10 for \( i > 1/2(11n - 10d) \),
(iv) if \( A_i > 0 \), then \( A_j = 0 \) for \( j > 11n - 10d - i \) and \( i \neq j \).

Proof. (I) (i) and (ii) are immediate from Lemma 2.
(iii) Suppose \( i > 1/2(7n - 6d) \). By part (i), there cannot be two linearly independent codeword of weight \( i \). So there are either no codeword of weight \( i \) or just six \((x, 2x, 3x, 4x, 5x \) and \( 6x \) for some \( x \in C \).
(iv) By part (i), there cannot exist codeword of weight \( i \) and \( j \), with \( i \neq j \), satisfying \( i + j > 7n - 6d \).

(II) The same way of (I). \(\square\)

**Definition 3.5.** Let \( C \) be an \([n, k, d]\)-code over \( GF(q) \). If we delete a given coordinate from all codewords of \( C \) then we have a punctured code of \( C \). This code is an \([n - 1, k, d - 1]\)-code. The set of all codewords of \( C \) having zero in a given coordinate position and then deleting that coordinate is a code called a shortened code of \( C \). This code is an \([n - 1, k - 1, d]\)-code, provided not the given position in all code words \( C \) is zero [9].

**Lemma 3.6.** [9] (i) \( n_q(k, d) \leq n_q(k, d + 1) - 1 \),
(ii) \( n_q(k, d) \geq n_q(k, d - 1) + 1 \),
(iii) \( n_q(k, d) \leq n_q(k + 1, d) - 1 \),
(iv) \( n_q(k, d) \geq n_q(k - 1, d) + 1 \).

**Definition 3.7.** Let \( G \) be the generator matrix of a linear \([n, k, d]\)-code \( C \) over \( GF(q) \). Then the residual code of \( C \) with respect to a codeword \( c \), denoted be \( \text{Res}(C, c) \), is the code generated by the restriction of \( G \) to the columns where \( c \) has a zero entry [9].

**Lemma 3.8.** [9] Suppose \( C \) is an \([n, k, d]\)-code over \( GF(q) \) and suppose \( c \in C \) has weight \( w \), where \( d > w(q - 1)/q \). Then \( \text{Res}(C, c) \) is an \([n - w, k - 1, d^0]\)-code with \( d^0 \geq d - w + \lceil w/q \rceil \).

([x] denotes the smallest integer greater than or equal to x.)

**Corollary 3.9.** Suppose \( C \) is an \([n, k, d]\)-code over \( GF(q) \), and let \( c \) be a codeword of weight \( d \). Then \( \text{Res}(C, c) \) is an \([n - d, k - 1, \lceil d/q \rceil]\)-code [9].

**Theorem 3.10.** (The Griesmer bound.) Let \( g_q(k, d) \) denote the sum expression \( \sum_{i=0}^{k-1} [d/q^i] \). Then \( n_q(k, d) \geq g_q(k, d) \).

The class of codes which satisfy the Griesmer bound is addressed as codes of type \( BV \). Such codes can be produced by certain puncturings of concatenations
of simplex codes and one can show that, for given \( q \) and \( k \), the Griesmer bound is attained for all sufficiently large \( d \). The following theorem gives a necessary and sufficient condition for the existence of a code of type \( BV[7,11,16] \).

**Theorem 3.11.** For given \( q, k \) and \( d \), write

\[
d = sq^{k-1} - \sum_{i=1}^{p} q^{u_i-1},
\]

where \( s = \lceil d/qk-1 \rceil \), \( k > u_1 \geq u_2 \geq \ldots \geq u_p \geq 1 \), and at most \( q-1 \) of \( u_i \)'s take any given value. Then there exists a \([g_q(k,d),k,d]\)-code of type \( BV \) if and only if

\[
\sum_{i=1}^{\min(s+1,p)} u_i \leq sk.
\]

4. Optimal Codes with \( q = 7,11 \) of Dimension \( \leq 3 \)

For \( k \leq 2 \), it follows from Theorem 11 that \( n_7(k,d) = g_7(k,d) \) for all \( d \). Thus \( n_7(1,d) = d \) and \( n_7(2,d) = d + \lceil d/7 \rceil \) for all \( d \).

For \( k = 3 \), Theorem 11 implies that \( n_7(3,d) = g_7(3,d) \) for \( d \geq 36 \). The remaining values of \( d \) are listed in Table 1.

<table>
<thead>
<tr>
<th>( d )</th>
<th>( g_7(3,d) )</th>
<th>( n_7(3,d) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>4</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>5</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>6</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>7</td>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>8</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>9</td>
<td>12</td>
<td>12</td>
</tr>
<tr>
<td>10</td>
<td>13</td>
<td>13</td>
</tr>
<tr>
<td>11</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>12</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>13</td>
<td>16</td>
<td>17</td>
</tr>
<tr>
<td>14</td>
<td>17</td>
<td>18</td>
</tr>
<tr>
<td>15</td>
<td>18</td>
<td>19</td>
</tr>
<tr>
<td>16</td>
<td>19</td>
<td>20</td>
</tr>
<tr>
<td>17</td>
<td>20</td>
<td>21</td>
</tr>
<tr>
<td>18</td>
<td>21</td>
<td>22</td>
</tr>
<tr>
<td>19</td>
<td>22</td>
<td>23</td>
</tr>
<tr>
<td>20</td>
<td>23</td>
<td>24</td>
</tr>
<tr>
<td>21</td>
<td>24</td>
<td>25</td>
</tr>
<tr>
<td>22</td>
<td>25</td>
<td>26</td>
</tr>
<tr>
<td>23</td>
<td>26</td>
<td>27</td>
</tr>
<tr>
<td>24</td>
<td>27</td>
<td>28</td>
</tr>
<tr>
<td>25</td>
<td>28</td>
<td>29</td>
</tr>
<tr>
<td>26</td>
<td>29</td>
<td>30</td>
</tr>
<tr>
<td>27</td>
<td>30</td>
<td>31</td>
</tr>
<tr>
<td>28</td>
<td>31</td>
<td>32</td>
</tr>
<tr>
<td>29</td>
<td>32</td>
<td>33</td>
</tr>
<tr>
<td>30</td>
<td>33</td>
<td>34</td>
</tr>
<tr>
<td>31</td>
<td>34</td>
<td>35</td>
</tr>
<tr>
<td>32</td>
<td>35</td>
<td>36</td>
</tr>
<tr>
<td>33</td>
<td>36</td>
<td>37</td>
</tr>
<tr>
<td>34</td>
<td>37</td>
<td>38</td>
</tr>
<tr>
<td>35</td>
<td>38</td>
<td>39</td>
</tr>
<tr>
<td>36</td>
<td>39</td>
<td>40</td>
</tr>
<tr>
<td>37</td>
<td>40</td>
<td>41</td>
</tr>
<tr>
<td>38</td>
<td>41</td>
<td>42</td>
</tr>
</tbody>
</table>

**Theorem 4.1.** (i) \( n_7(3,5) \leq 7 \), (ii) \( n_7(3,6) \leq 8 \), (iii) \( n_7(3,11) \leq 14 \).
Proof. (i) The matrix 
\[
\begin{pmatrix}
0 & 4 & 3 & 2 & 0 & 3 & 1 \\
6 & 0 & 0 & 3 & 2 & 1 & 3 \\
5 & 2 & 4 & 2 & 1 & 5 & 1
\end{pmatrix}
\]
generates \([7, 3, 5]\)-code over \(GF(7)\).

(ii) It is shown in [11] that \([q + 1, 3, q - 1]\)-code exists over \(GF(q)\). In particular, there exists \([8, 3, 6]\)-code over \(GF(7)\). Its generator matrix is 
\[
\begin{pmatrix}
4 & 4 & 3 & 2 & 1 & 0 & 3 & 0 \\
4 & 0 & 1 & 5 & 4 & 3 & 6 & 0 \\
5 & 6 & 3 & 5 & 0 & 0 & 5 & 1
\end{pmatrix}
\]

(iii) The matrix 
\[
\begin{pmatrix}
1 & 3 & 2 & 1 & 1 & 1 & 2 & 3 & 0 & 1 & 3 & 1 & 3 & 3 \\
5 & 0 & 4 & 1 & 5 & 2 & 5 & 5 & 0 & 1 & 2 & 6 & 2 & 5 \\
2 & 1 & 2 & 6 & 3 & 4 & 6 & 4 & 4 & 1 & 1 & 6 & 2 & 3
\end{pmatrix}
\]
generates \([14, 3, 11]\)-code over \(GF(7)\) and its weight distribution is 
\[A_{11} = 162, \quad A_{12} = 60, \quad A_{13} = 66, \quad A_{14} = 54.\] □

Theorem 4.2. \(n_7(3, 10) \leq 13\).

Proof. The matrix 
\[
\begin{pmatrix}
0 & 6 & 1 & 6 & 2 & 5 & 1 & 0 & 1 & 5 & 0 & 6 & 2 \\
2 & 4 & 6 & 3 & 1 & 6 & 1 & 6 & 1 & 2 & 2 & 1 & 4 \\
2 & 1 & 4 & 3 & 2 & 4 & 2 & 1 & 3 & 2 & 0 & 6 & 3
\end{pmatrix}
\]
generates \([13, 3, 10]\)-code over \(GF(7)\) and its weight distribution is 
\[A_{10} = 126, \quad A_{11} = 90, \quad A_{12} = 66, \quad A_{13} = 60.\] □

Theorem 4.3. (i) \(n_7(3, 7) > 9\), (ii) \(n_7(3, 35) > 41\).

Proof. (i) If \(q\) is odd, an \([q + k - 1, k]\)-code MDS does not exist [1]. Then \([9, 3, 7]\)-code does not exist. This matrix generates \([10, 3, 7]\)-code with weight distribution 
\[A_7 = 54, \quad A_8 = 108, \quad A_9 = 102, \quad A_{10} = 78\]
\[
\begin{pmatrix}
3 & 1 & 1 & 3 & 1 & 2 & 0 & 1 & 1 & 4 \\
2 & 6 & 3 & 6 & 5 & 0 & 1 & 6 & 5 & 6 \\
1 & 4 & 1 & 6 & 6 & 0 & 0 & 1 & 0 & 6
\end{pmatrix}
\]

(ii) For \(d = (k - 2)q^{k-1} - (k - 1)q^{k-2}\), \(n_q(k, d) > g_q(k, d)\) holds for \(q \geq k\), \(k = 3, 4, 5\) [12]. Then we have for \(k = 3\) and \(q = 7\), \([41, 3, 35]\)-code does not exist. □

Theorem 4.4. \(n_7(3, 13) > 16\).

Proof. Suppose, for a contradiction, that there exist a \([16, 3, 13]\)-code \(C\) over \(GF(7)\). Since there do not exist codes over \(GF(7)\) with parameters \([15, 3, 13]\) and \([14, 2, 13]\), it follows from Lemma 2 that \(B_1 = B_2 = 0\). The first three MacWilliams identities (Theorem 1) become, 
\[A_{13} + A_{14} + A_{15} + A_{16} = 342,\]
\[A_{14} + 2A_{15} + 3A_{16} = 258,\]
A_{15} + 3A_{16} = 210.

By Lemma 8, the residual code of C with respect to a codeword of weight 15 would be a [1, 2, 1]-code, which does not exist, so A_{15} = 0. Bearing in mind that each A_i must be a nonnegative integer multiple of 6 (because if x is a nonzero codeword, then so also are 2x, 3x, 4x, 5x and 6x of the same weight). The last equation gives A_{16} = 70 that is not divisible by 6.

This matrix generates [17, 3, 13]-code

\[
\begin{pmatrix}
4 & 6 & 0 & 4 & 5 & 5 & 5 & 1 & 6 & 6 & 4 & 1 & 0 & 6 & 5 \\
2 & 6 & 4 & 5 & 0 & 2 & 5 & 6 & 0 & 5 & 5 & 1 & 2 & 1 & 2 & 3 & 3 \\
6 & 1 & 5 & 3 & 3 & 6 & 1 & 2 & 6 & 3 & 2 & 5 & 2 & 5 & 4 & 5 & 3
\end{pmatrix}
\]

and its weight distribution is A_{13} = 60, A_{14} = 126, A_{15} = 78, A_{16} = 42 and A_{17} = 36.

\[\square\]

**Theorem 4.5.** \(n_{7}(3, 21) > 25\).

**Proof.** Suppose there exist an [25, 3, 21]-code C over GF(7). By Lemma 2, B_1 = B_2 = 0. The MacWilliams identities become,

(a) \(A_{21} + A_{22} + A_{23} + A_{24} + A_{25} = 342\),
(b) \(A_{22} + 2A_{23} + 3A_{24} + 4A_{25} = 168\),
(c) \(A_{23} + 3A_{24} + 6A_{25} = 252\).

By Lemma 8, \(A_{22} = A_{23} = A_{24} = 0\). By Corollary 4(iii), \(A_{25} = 0\) or 6, this contradicts (c).

This matrix generates [26, 3, 21]-code and its weight distribution is \(A_{21} = 108, A_{22} = 108, A_{23} = 60, A_{24} = 42, A_{25} = 12\) and \(A_{26} = 12\).

\[\square\]

**Theorem 4.6.** \(n_{7}(3, 28) > 33\).

**Proof.** Suppose there exist an [33, 3, 28]-code C over GF(7). By Lemma 2, B_1 = B_2 = 0. The MacWilliams identities become,

(a) \(A_{28} + A_{29} + A_{30} + A_{31} + A_{32} + A_{33} = 342\),
(b) \(A_{29} + 2A_{30} + 3A_{31} + 4A_{32} + 5A_{33} = 126\),
(c) \(A_{30} + 3A_{31} + 6A_{32} + 10A_{33} = 252\),

By Lemma 8, \(A_{29} = A_{30} = A_{31} = A_{32} = 0\). By Corollary 4(iii), \(A_{33} = 0\) or 6, which contradicts (c).

\[\square\]

**Theorem 4.7.** (i) \(n_{11}(3, 5) \leq 7\), (ii) \(n_{11}(3, 7) \leq 9\), (iii) \(n_{11}(3, 13) \leq 16\), (iv) \(n_{11}(3, 14) \leq 17\).

**Proof.** (i) This matrix generates [7, 3, 5]-code and its weight distribution is \(A_5 = 210, A_6 = 420\) and \(A_7 = 700\).

\[
\begin{pmatrix}
3 & 9 & 10 & 0 & 9 & 3 & 4 \\
6 & 9 & 5 & 3 & 8 & 10 & 9 \\
7 & 1 & 6 & 4 & 8 & 9 & 4
\end{pmatrix}
\]
This matrix generates $[9, 3, 7]$-code and its weight distribution is $A_7 = 360$, $A_8 = 360$ and $A_9 = 610$. Another generator matrix is given in section 4.

\[
\begin{pmatrix}
10 & 4 & 5 & 1 & 1 & 1 & 3 & 8 \\
1 & 9 & 7 & 1 & 1 & 0 & 8 & 0 \\
2 & 1 & 10 & 2 & 4 & 6 & 9 & 9 \\
\end{pmatrix}
\]

(iii) The matrix

\[
\begin{pmatrix}
0 & 2 & 1 & 10 & 9 & 1 & 10 & 6 & 4 & 5 & 2 & 3 & 0 & 5 & 10 & 4 \\
1 & 4 & 10 & 1 & 7 & 2 & 4 & 6 & 0 & 3 & 2 & 3 & 5 & 2 & 6 & 6 \\
4 & 7 & 5 & 3 & 9 & 5 & 9 & 2 & 10 & 1 & 6 & 0 & 7 & 6 & 4 & 9 \\
\end{pmatrix}
\]

generates $[16, 3, 13]$-code over $GF(11)$ and its weight distribution is $A_{13} = 300$, $A_{14} = 300$, $A_{15} = 420$ and $A_{16} = 310$.

(iv) The matrix

\[
\begin{pmatrix}
3 & 6 & 0 & 1 & 8 & 10 & 8 & 3 & 3 & 2 & 5 & 4 & 4 & 5 & 6 & 3 & 3 \\
6 & 6 & 7 & 8 & 4 & 5 & 2 & 8 & 0 & 8 & 10 & 1 & 9 & 2 & 7 & 9 \\
3 & 4 & 9 & 1 & 8 & 1 & 3 & 2 & 5 & 8 & 7 & 1 & 0 & 10 & 7 & 6 & 6 \\
\end{pmatrix}
\]

generates $[17, 3, 14]$-code over $GF(11)$ and its weight distribution is $A_{14} = 340$, $A_{15} = 340$, $A_{16} = 340$ and $A_{17} = 310$.

5. Quasi-Cyclic Codes

QC codes are a generalization of cyclic codes whereby a cyclic shift of a codeword by $p$ positions results in another codewords. It can be shown that $p$ must be divisor of $n$ [8]. Therefore, cyclic codes are QC codes with $p = 1$. With a suitable permutation of coordinate, many QC codes can be characterized in terms of $m \times m$ circulant matrices, so the blocklength, $n$, is a multiple of $m$, $n = mp$. The generator matrix can then be represented as $G = [C_0, C_1, C_2, \ldots, C_{p-1}]$. $C_i$ is an $m \times m$ circulant matrix of the form

\[
C = \begin{pmatrix}
  c_0 & c_1 & c_2 & \cdots & c_{m-1} \\
  c_{m-1} & c_0 & c_1 & \cdots & c_{m-2} \\
  c_{m-2} & c_{m-1} & c_0 & \cdots & c_{m-3} \\
  \vdots & \vdots & \vdots & \ddots & \vdots \\
  c_1 & c_2 & c_3 & \cdots & c_0 \\
\end{pmatrix}
\]

where each successive row is a right cyclic shift of the previous one. These codes are a subclass of the more general $1$-generator QC codes [20], which is in turn a subclass of all QC codes.

This has been confined mainly to the case $m = k$. An $s$-QC $[sk, k]$-codes has a generator matrix of the form $G = [G_1 \mid G_2 \mid \cdots \mid G_s]$, where each $G_i$ is a $k \times k$ circulant matrix. The matrix $G_1$ is usually taken to be the identity matrix $I$ [8]. In this section we produce generator matrix of QC $[sk, k]$-codes with $k = 3$ over $GF(7)$ and $GF(11)$.

Theorem 5.1. (i) $n_7(3, 4) = 6$, (ii) $n_7(3, 9) = 12$, (iii) $n_7(3, 12) = 15$, (iv) $n_7(3, 14) = 18$. 

Proof. There exist codes with parameters [6, 3, 4], [12, 3, 9], [15, 3, 12] and [18, 3, 14]-codes. The weight distributions and generators matrices are:

\[ [6, 3, 4] \quad A_0 = 1, A_4 = 90, A_5 = 108 \text{ and } A_6 = 144; \]
\[ (422 \mid 533); \]
\[ [12, 3, 9] \quad A_0 = 1, A_9 = 102, A_{10} = 90, A_{11} = 90 \text{ and } A_{12} = 60; \]
\[ (322 \mid 633 \mid 022 \mid 046); \]
\[ [12, 3, 9] \quad A_0 = 1, A_9 = 96, A_{10} = 108, A_{11} = 72 \text{ and } A_{12} = 66; \]
\[ (532 \mid 066 \mid 212 \mid 040); \]
\[ [15, 3, 12] \quad A_0 = 1, A_{12} = 180, A_{13} = 90, A_{14} = 0 \text{ and } A_{15} = 72; \]
\[ (205 \mid 021 \mid 642 \mid 054 \mid 346); \]
\[ [18, 3, 14] \quad A_0 = 1, A_{14} = 90, A_{15} = 90, A_{16} = 108, A_{17} = 18 \text{ and } A_{18} = 36; \]
\[ (322 \mid 633 \mid 022 \mid 046 \mid 450 \mid 244); \]
\[ [18, 3, 14] \quad A_0 = 1, A_{14} = 90, A_{15} = 108, A_{16} = 54, A_{17} = 72 \text{ and } A_{18} = 18; \]
\[ (515 \mid 212 \mid 343 \mid 531 \mid 630 \mid 500). \]

\[ \square \]

Theorem 5.2. (i) \( n_7(3, 17) = 21 \), (ii) \( n_7(3, 19) = 24 \), (iii) \( n_7(3, 22) = 27 \) and (iv) \( n_7(3, 27) = 33 \).

Proof. There exist codes with parameters [21, 3, 17], [24, 3, 19], [27, 3, 22] and [33, 3, 27] codes. The weight distributions and generators matrices are:

\[ [21, 3, 17] \quad A_0 = 1, A_{17} = 126, A_{18} = 168, A_{19} = 0, A_{20} = 0 \text{ and } A_{21} = 48; \]
\[ (002 \mid 521 \mid 321 \mid 640 \mid 434 \mid 633 \mid 624); \]
\[ [24, 3, 19] \quad A_0 = 1, A_{19} = 72, A_{20} = 108, A_{21} = 90, A_{22} = 18, A_{23} = 54 \text{ and } A_{24} = 0; \]
\[ (255 \mid 520 \mid 452 \mid 045 \mid 423 \mid 544 \mid 546 \mid 202); \]
\[ [24, 3, 19] \quad A_0 = 1, A_{19} = 108, A_{20} = 36, A_{21} = 84, A_{22} = 108, A_{23} = 0 \text{ and } A_{24} = 6; \]
\[ (164 \mid 566 \mid 346 \mid 114 \mid 110 \mid 311 \mid 552 \mid 034); \]
\[ [27, 3, 22] \quad A_0 = 1, A_{22} = 126, A_{23} = 90, A_{24} = 102, A_{25} = 0, A_{26} = 0 \text{ and } A_{27} = 24; \]
\[ (646 \mid 623 \mid 565 \mid 101 \mid 354 \mid 136 \mid 605 \mid 130 \mid 043); \]
\[ [33, 3, 27] \quad A_0 = 1, A_{27} = 96, A_{28} = 126, A_{29} = 54, A_{30} = 42, A_{31} = 18, A_{32} = 0 \text{ and } A_{33} = 6; \]
\[ (245 \mid 664 \mid 023 \mid 432 \mid 513 \mid 404 \mid 056 \mid 104 \mid 543 \mid 051 \mid 246); \]
\[ [33, 3, 27] \quad A_0 = 1, A_{27} = 54, A_{28} = 216, A_{29} = 18, A_{30} = 24, A_{31} = 18, A_{32} = 0 \text{ and } A_{33} = 12; \]
\[ (426 \mid 210 \mid 060 \mid 533 \mid 461 \mid 105 \mid 453 \mid 552 \mid 242 \mid 305 \mid 022). \]

\[ \square \]

Theorem 5.3. (i) \( n_7(3, 30) = 36 \), (ii) \( n_7(3, 32) = 39 \) and (iii) \( n_7(3, 35) = 42 \).

Proof. There exist codes with parameters [36, 3, 30], [39, 3, 32] and [42, 3, 35] codes. The weight distributions and generators matrices are:

\[ [36, 3, 30] \quad A_0 = 1, A_{30} = 108, A_{31} = 90, A_{32} = 54, A_{33} = 6, A_{34} = 18, A_{35} = 0 \text{ and } A_{36} = 6; \]
\[ (515 \mid 146 \mid 605 \mid 153 \mid 130 \mid 200 \mid 012 \mid 253 \mid 302 \mid 251 \mid 411 \mid 434); \]
Proof. Theorem 5.4.

(i) $n_{11}(3,4) = 6$, (ii) $n_{11}(3,7) = 9$ and (iii) $n_{11}(3,10) = 12$.

Proof. There exist codes with parameters $[6,3,4]$, $[9,3,7]$ and $[12,3,10]$ codes. The weight distributions and generator matrices are:

$[6,3,4]$ - $A_0 = 1$, $A_4 = 150$, $A_5 = 420$ and $A_6 = 760$;
(5 2 7 | 10 3 4);

$[9,3,7]$ - $A_0 = 1$, $A_7 = 360$, $A_8 = 360$ and $A_9 = 610$;
(9 1 8 | 4 1 3 | 5 6 5);

$[12,3,10]$ - $A_0 = 1$, $A_{10} = 660$, $A_{11} = 120$ and $A_{12} = 550$;
(3 6 10 | 6 6 9 | 4 6 8 | 5 5 10).

Theorem 5.5.

(i) $n_{11}(3,12) = 15$, (ii) $n_{11}(3,15) = 18$ and (iii) $n_{11}(3,18) = 21$.

Proof. There exist codes with parameters $[15,3,12]$, $[18,3,15]$ and $[21,3,18]$ codes. The weight distributions and generator matrices are:

$[15,3,12]$ - $A_0 = 1$, $A_{12} = 210$, $A_{13} = 420$, $A_{14} = 330$ and $A_{15} = 370$;
(7 10 4 | 6 4 10 | 0 10 4 | 2 6 5 | 6 7 6);
Optimal Linear Codes Over $GF(7)$ and $GF(11)$ with Dimension 3

[18, 3, 15] - $A_0 = 1$, $A_{15} = 400$, $A_{16} = 330$, $A_{17} = 300$ and $A_{18} = 300$;
(0 4 8 | 0 3 3 | 3 9 9 | 1 8 2 | 8 2 5 | 1 6 1);
[21, 3, 18] - $A_0 = 1$, $A_{18} = 630$, $A_{19} = 210$, $A_{20} = 210$ and $A_{21} = 280$;
(6 2 1 | 1 1 2 | 1 5 4 | 8 10 10 | 2 0 9 | 7 1 10 | 8 6 1).

Theorem 5.6. (i) $n_{11}(3, 27) = 23$, (ii) $n_{11}(3, 26) = 30$ and (iii) $n_{11}(3, 34) = 39$.

The weight distributions and generators matrices are:
[27, 3, 23] - $A_0 = 1$, $A_{23} = 390$, $A_{24} = 280$, $A_{25} = 330$, $A_{26} = 180$ and $A_{27} = 150$;
(10 5 1 | 0 5 3 | 2 1 7 | 10 1 4 | 2 0 9 | 2 7 9 | 2 5 7 | 2 6 1 | 9 10 6);
[30, 3, 26] - $A_0 = 1$, $A_{26} = 540$, $A_{27} = 300$, $A_{28} = 210$, $A_{29} = 120$;
(9 4 4 | 2 4 9 | 10 0 8 | 3 3 0 | 8 4 3 | 0 9 6 | 7 6 4 | 2 3 7 | 10 2 3 | 8 6 1);
[39, 3, 34] - $A_0 = 1$, $A_{34} = 450$, $A_{35} = 360$, $A_{36} = 220$, $A_{37} = 90$, $A_{38} = 150$ and $A_{39} = 60$;
(5 3 6 | 4 4 0 | 2 9 3 | 2 6 1 | 4 5 3 | 1 1 4 | 5 9 2 | 9 7 9 | 6 10 8 | 3 7 10 | 7 1 3 | 3 5 7 | 3 8 6).

The authors would like to give their best thanks to the anonymous referee for his/her valuable comments to promote this work.

Acknowledgments

The authors would like to give their best thanks to the anonymous referee for his/her valuable comments to promote this work.

References