A NOTE ON COVERING RADIUS OF MacDonald CODES

M.C.Bhandari
Department of Mathematics,
Indian Institute of Technology Kanpur,
Kanpur, 208016(India)
mcb@iitk.ac.in

C.Durairajan,
Government Arts College,
Musiri, Tamilnadu(India)

Abstract

In this paper we determine an upper bound for the covering radius of a q-ary MacDonald code $C_{k,u}(q)$. Values of $n_q(4,d)$, the minimal length of a 4-dimensional q-ary code with minimum distance $d$ is obtained for $d = q^2 - 1$ and $q^2 - 2$. These are used to determine the covering radius of $C_{3,1}(q), C_{3,2}(q)$ and $C_{4,2}(q)$.

Theorem 7 of the present paper gives a nice upper bound for the covering radius of a MacDonald code $C_{k,u}(q)$. Values of $n_q(4,d)$ are determined for (a) $1 \leq i \leq 3$ and $q$ odd. These are used to determine the covering radius of $C_{3,1}(q), C_{3,2}(q)$ and $C_{4,2}(q)$.

Index Terms: Linear Codes, Covering radius, MacDonald codes, Optimal codes.

Let $F_q = \{0, 1, \alpha, \ldots, \alpha^{q-1}\}$ be a Galois field. An $[n,k,d]$ code $C$ is a $k$-dimensional subspace of $F_q^n$ having minimum Hamming distance $d$. One of the central problem in coding theory is to determine $n_q(k,d)$, the minimal value of $n$ for which an $[n,k,d]$ code exists. In 1960 Solomon and Stiffler showed that

$$n_q(k,d) \geq \sum_{i=0}^{k-1} \left\lfloor \frac{d}{q^i} \right\rfloor \equiv g_q(k,d), \quad (1)$$

where $\lceil x \rceil$ denotes the least integer greater than or equal to $x$ [1]. For binary codes the above bound was first proved by Griesmer [2] and is called the Griesmer bound. An $[n_q(k,d), k,d]$ code is called an optimal code. Well known examples of codes that meet the Griesmer bound are simplex codes $S_k(q)$ and MacDonald codes $C_{k,u}(q)$. The covering radius of a code $C$ is the weight of a maximum weight coset leader. Determining covering radius of a code in general is a difficult task. Many lower and upper bounds have been obtained [3], [4]. Very little is known about the covering radius of simplex codes [5] and almost nothing is known about the covering radius of MacDonald codes.

Theorem 7 of the present paper gives a nice upper bound for the covering radius of a MacDonald code $C_{k,u}(q)$. Values of $n_q(4,d)$ are determined for (a) $1 \leq i \leq 2$ and $d \leq q - 1$ and $q$ odd. These are used to determine the covering radius of $C_{3,1}(q), C_{3,2}(q)$ and $C_{4,2}(q)$.

The bound given by Theorem 7 is further improved for $u = 2$ (Corollary 15) and for $u = 1$ and $q = 3$ (Theorem 16).

It is shown that $R(S_4(3)) = 24$, $R(C_{4,2}(3)) = 23$ and $21 \leq R(C_{4,2}(3)) \leq 22$.

The covering radius of an $[n,1,n]$ repetition code is $n - \lfloor \frac{d}{q} \rfloor$ [5]. If $C_0$ and $C_1$ are binary codes generated by the matrices $G_0$ and $G_1$ respectively and if $C$ is the code generated by the matrix

$$G = \left[ \begin{array}{c|c} 0 & G_1 \\ \hline G_0 & \end{array} \right],$$

then Mattson [4] has shown that

$$R(C) \leq R(C_0) + R(C_1). \quad (2)$$

If in addition $dim(C_0) \geq dim(C_1)$ and $D$ is the code generated by the matrix

$$\left[ \begin{array}{c} G_0 \\ \hline G_1 \end{array} \right],$$

then

$$R(D) \geq R(C_0) + R(C_1). \quad (3)$$

The proof of both of these results easily extend to q-ary codes. Best known upper bound for the covering radius of an optimal code is given by the following theorem.

**THEOREM 1 (6):** The covering radius of an $[n_q(k,d), k,d]$ code is at most $d - b_q(k,d)$, where $b_q(k,d) = n_q(k+1,d) - n_q(k,d)$. Moreover if $b_q(k,d) = 1$, then there exists an $[n_q(k,d), k,d]$ code with covering radius $d - 1$.

Values of $n_q(3,d)$ for $d \leq q + 1$ are given by the following theorem of Dodunekov.

**THEOREM 2 (7):** (i) If $q$ is even, $q \geq 4$, then $n_q(3,d) = g_q(3,d)$ for all $d \leq q + 2$. (ii) If $q$ is odd then

$$n_q(3,d) = \begin{cases} g_q(3,d), & d \leq q - 1 \text{ or } d = q - 1 \\ g_q(3,d) + 1, & d = q. \end{cases} \quad (4)$$
A nice way of constructing new codes from a given code C is by considering residual codes of C. If C has a code word c of weight w then the code obtained from C by considering only those coordinates in which c has 0 is called a residual code and is denoted by Res(C, w). If \( w < d + \left[ \frac{w}{2} \right] \), then Res(C, w) is an \([n - w, k - 1, d + 1]_C\) code with \( d + 1 \geq d - w + \left[ \frac{w}{2} \right] \).

For each i, let \( A_i \) and \( B_i \) be the number of codewords of weight i in C and \( C^* \) (dual code of C), respectively. The sequence \( \{ A_i \}_{i=0}^{n} \) is called the weight distribution of C. \( A_i \)'s and \( B_i \)'s are related by the equations

\[
\sum_{j=0}^{n-i} \binom{n - j}{t} A_j = q^{k-t} \sum_{j=0}^{t} \binom{n - j}{n-t} B_j, \quad (5)
\]

for \( t = 0, 1, \ldots, n \) and are called MacWilliams identities [8]. If \( u \) and \( v \) are linearly independent elements in \( F_q^* \) then Hill and Newton [8] have shown that

\[
wt(u) + wt(v) + \sum_{\lambda \in F_q \setminus \{0\}} wt(u + \lambda v) = q(n - z) \quad (6)
\]

where \( z \) denotes the number of coordinate places in which both \( u \) and \( v \) have zero entries.

The following two lemmas give results on codes that meet the Griesmer bound.

**Lemma 3** ([7]) \(-\): If \( q \) divides \( d \) and \( n_q(k, d) = g_q(k, d) \) then \( n_q(k, d - a) = g_q(k, d - a) \) for all \( 1 \leq a \leq q - 1 \). Conversely, if \( q \) divides \( d \) and \( n_q(k, d - a) > g_q(k, d - a) \) for some \( 1 \leq a \leq q - 1 \), then \( n_q(k, d - b) > g_q(k, d - b) \) for all \( 0 \leq b \leq a \).

**Lemma 4** ([8]) \(-\): Suppose \( C \) is an \([n, k, d]_C\) code which meets the Griesmer bound and suppose \( j \) is a positive integer such that \( d \leq q^{k-j+1} \). Then \( B_j = 0 \).

Let \( S_k(q) \) be a \([q^k - 1/(q - 1), k, q^{k-1}] \) simplex code and let \( G_1(q) \) be a generator matrix of \( S_k(q) \). Then columns of \( G_k(q) \) are pairwise linearly independent k-tuples over \( GF(q) \). Moreover, any two such matrices generate equivalent codes. If \( k = 2 \) then

\[
G_2(q) = \begin{bmatrix}
0 & 1 & 1 & \cdots & \cdots & 1 \\
1 & 0 & 1 & \alpha_3 & \cdots & \alpha_q
\end{bmatrix}
\]

By induction, it is easy to see that

\[
G_k(q) = \begin{bmatrix}
\alpha_q & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 1 & \cdots & \cdots & 1 \\
1 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 1 & \cdots & \cdots & 1 \\
\vdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \vdots & \cdots & \cdots & \vdots \\
0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & \cdots & \cdots & 0
\end{bmatrix}
\]

is a generator matrix for \( S_k(q) \).

Consider the code \( C_{k, u}(q); 1 \leq u \leq k - 1 \) generated by the matrix

\[
G_{k, u}(q) = \left[ G_k(q) \setminus \left( \begin{array}{c}
0 \\
G_u(q)
\end{array} \right) \right] \quad (7)
\]

where \( 0 \) is a \((k - u) \times (q^n - 1)/(q - 1) \) zero matrix and \([A \setminus B] \) denotes the matrix obtained from \( A \) by deleting the columns of \( B \). For \( q = 2 \) these codes were introduced by MacDonald [9]. For \( q \geq 3 \) these codes are defined in [10] to solve a classical combinatorial problem. The code \( C_{k, u}(q) \) is a \([q^k - q^{u+1}]/(q - 1), k, q^{k-1} - q^{u-1}] \) code that meets the Griesmer bound and is called a MacDonald code. In [11], Garg has determined the covering radius of binary MacDonald codes \( C_{k, 1}(2) \) and \( C_{k, 2}(2) \). He has also obtained lower and upper bounds for the covering radius of \( C_{k, u}(2) \) in general but they are far from the exact value. We observe that

\[
G_{k, u}(q) = \begin{bmatrix}
G_{k, k-1}(q) & G_{k-1, u}(q)
\end{bmatrix}
\]

and hence by (3)

\[
R(C_{k, u}(q)) \geq R(C_{k, k-1}(q)) + R(C_{k-1, u}(q)) \quad (8)
\]

If \( u < m \leq k - 1 \), the following lemma gives a relation between \( R(C_{k, u}(q)) \) and \( R(C_{m, u}(q)) \).

**Lemma 5** \(-\):

\[
R(C_{k, u}(q)) \leq q^{k-1} - q^{u-1} + R(C_{m, u}(q)) \quad (9)
\]

In particular if \( m = u + 1 \), the above lemma gives

\[
R(C_{k, u}(q)) \leq q^{k-1} - q^u + R(C_{u+1, u}(q)) \quad (10)
\]

**Lemma 6** \(-\):

If \( u \geq 3 \) then \( R(C_{u+1, u}(q)) \leq q^u - q^{u-1} - 2 \).

Proof:- Let \( u \geq 3 \). Since \( C_{u+1, u}(q) \) is an optimal code, \( R(C_{u+1, u}(q)) \leq q^u - q^{u-1} - 1 \). If \( R(C_{u+1, u}(q)) = q^u - q^{u-1} - 1 \), then there exists \( g \in F_q^* \) with \( d(g, C_{u+1, u}(q)) = q^u - q^{u-1} - 1 \). Let \( C \) be the \([q^u + 1, u + 2, q^u - q^{u-1}] \) code generated by the matrix
Then $A_w = 0$ for each $w = q^u - q^{u-1} + i; 1 \leq i \leq q^{u-1} - 1$. For if $A_w \neq 0$ for some $i$ then Res($C, w$) is a $[q^{u-1} + 1 - i, u + 1, q^{u-1} - q^{u-2} + \lfloor \frac{1}{q} \rfloor - 1]$ code. But such a code does not exist as its parameters do not satisfy the Griesmer bound given by (1). Therefore possible nonzero weights in $C$ are $d = q^u - q^{u+1}, n - 1$ and $n = q^{u} + 1$. Since $q^u - q^{u-1} \leq q^{u-1}$ and the code $C$ meets the Griesmer bound, by Lemma 4 $B_1 = B_2 = 0$. The MacWilliams identities (5) gives

$$A_d + A_{n-1} + A_n = q^{u+2} - 1$$

$$(q^{u+1} + 1)A_d + A_{n-1} = (q^{u+1} - 1)n$$

$$(q^{u+1} + 1)q^{u+1}/2A_d = (q^{u} - 1)n(n-1)/2$$

solving these equations we get $A_n = (q - 1)q^{u+1}(1 - q^{u-2})/(q^{u+1} - 1) < 0$, a contradiction. Hence $R(C_{u+1}, u(q)) \leq q^{u-1} - 2$.

Replacing $R(C_{u+1}, u(q))$ in (8) by the bound obtained above we get the following upper bound for the covering radius of $C_{k,u(q)}$.

**THEOREM 7** : If $u \geq 3$ then $R(C_{k,u(q)} \leq q^{k-1} - q^{u-1} - 2$.

**Corollary 8** $R(C_{4,3}(3)) = 16$

Proof:- Let $C$ be the [29,5,18] ternary code with two equal co-ordinate constructed by VanEupen [13,Example 1]. A generator matrix for $C$ can be written in the form

$$G = \begin{bmatrix} y & 1 & \cdots & 0 \\ G_{u+1,u(q)} & - & \cdots & - \\ 0 & - & \cdots & - \\ \end{bmatrix}$$

Then the matrix $G_1$ generates a [27,4,18] ternary code $C_1$ and $d(x, C_1) = 16$. Therefore $R(C_{4,3}(3)) \geq 16$ and hence by theorem 7, $R(C_{4,3}(3)) = 16$.

**THEOREM 9** : $R(C_{2,1}(q)) = q - 2$ and $R(C_{3,2}(q)) = q^2 - q - 1$.

Proof:- In [12], Calderbank has shown that $n_3(q, q^2 - q) = q^2 + 1$. Therefore $b_3(2, q - 1) = 1$ and hence by theorem 1, there exists a $[q^2, 3, q^2 - q]$ code with covering radius $q^2 - q - 1$. Since equivalent codes have same covering radius, $R(C_{2,1}(q)) = q^2 - q - 1$. Similarly, by Theorem 2, $b_4(2, q - 1) = 1$ and hence by Theorem 1, $R(C_{2,1}(q)) = q - 2$.

We need the values of $n(q, q^2 - 1)$ and $n(q, q^2 - 2)$ for determining $R(C_{3,1}(q))$ and $R(C_{4,2}(q))$.

**THEOREM 10** : If $q \geq 3$ then $n(q, q^2 - i) = g_3(q, q^2 - i) + 1$ for $i = 1$ and 2.

Proof:- Let $A$ be the $[q^2 + 1, 4, q^2 - q]$ q-ary two weight code with $A_{4,2} \neq 0$ constructed in [12]. It has a generator matrix of the form

$$G_A = \begin{bmatrix} 0 & 1 & \cdots & 1 \\ 1 & 0 & x' & 0 \\ 0 & x' & 0 & 0 \\ \end{bmatrix}$$

Let $1 \leq i \leq q - 1$ and let $B$ be a $[q + 2 - i, 3, q - i]$ code. Then $B$ has a generator matrix of the form

$$G_B = \begin{bmatrix} 1 & y \\ 0 & y' \\ 0 & y'' \\ \end{bmatrix}$$

and

$$G = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ G_B & G_A \\ \end{bmatrix}$$

generates a $[q^2 + q + 3 - i, 4, q^2 - i]$ code. Therefore

$$n(q, q^2 - i) \leq g_4(q, q^2 - i) + 1 \text{ for } 1 \leq i \leq q - 1$$

If $n(q, q^2 - 2) = q^2 + q = n$ and $d = q^2 - 2$, let $C$ be a [n, 4, d] code. Then $3 \leq i \leq q$ and let $w = d + i$. If $A_w \neq 0$ for some $i$, then Res$(C, w)$ is an $[n - w, 3, q + \lfloor \frac{(i-2)}{q} \rfloor]$ code. But such a code does not exist as its parameter do not satisfy (1). Hence possible nonzero weights in $C$ are $d, d + 1, d + 2, n - 1$ and $n$. By Lemma 4, $B_j = 0$ for $j = 1, 2, 3$. The MacWilliams identities (5) gives

$$A_d + A_{d+1} + A_{d+2} + A_{n-1} + A_n = q^4 - 1$$

$$(q + 2)A_d + (q + 1)A_{d+1} + qA_{d+2} + A_{n-1} = (q^2 - 1)n$$

$$(q + 2)(q + 1)A_d + (q + 1)qA_{d+1} + q(q - 1)A_{d+2} = (q^2 - 1)n(n - 1)$$

$$(q + 2)(q + 1)qA_d + (q + 1)q(q - 1)A_{d+1} + q(q - 1)(q - 2)A_{d+2} = (q - 1)n(n - 1)(n - 2)$$

By (6), one of $A_n$ and $A_{n-1}$ must be zero. Moreover if $A_n \neq 0$ then $A_n = q - 1$. If $q \geq 3$, $A_n = q - 1$ and $A_{n-1} = 0$, then solving above equations we get $A_{d+1} < 0$, a contradiction. Hence $A_n = 0$. Solving above equations again we get $A_{d+2} < 0$, a contradiction. Therefore $n(q, q^2 - 2) \geq q^2 + q + 1 = g_3(q, q^2 - 2) + 1$ and hence
If \( n_q(4,q^2 - i) \) with \( q \geq 3 \).

Therefore by (11) and (12), \( n_q(4,q^2 - i) = g_q(4,q^2 - i) + 1 \) for \( i = 1, 2 \).

If \( q \) is odd then (12) is also true for \( 3 \leq i \leq q - 1 \). If \( n_q(4,q^2 - i) = g_q(4,q^2 - i) \) for some \( i, 3 \leq i \leq q - 1 \) then there exists a \([q^2 + q + 2 - i,q^2 - i] \) code \( C \) and hence \( \text{Res}(C,q^2 - i) \) is a \([q + 2, 3, q] \) code which does not exist. Thus using (12) we have,

**THEOREM 11** :- If \( q \) is odd then \( n_q(4,q^2 - i) = g_q(4,q^2 - i) + 1 \) for \( 1 \leq i \leq q - 1 \).

**THEOREM 12** :- \( R(C_{3,1}(q)) = q^3 - 3 \).

Proof:- Let \( x, x', x'', y, y', y'' \) be as defined in (10) and (11) for \( i = 1 \) and let \( C \) be the \([q^2 + q,3,q^2 - 1] \) code generated by the matrix

\[
G' = \left[ \begin{array}{cc|ccc} x' & y' & x'' & y'' & 0 \end{array} \right].
\]

Since \( d(x,y,C) = q^2 - 3; R(C) = q^2 - 3 \). If \( R(C) = q^2 - 2 \) then there exists \( z \in F_q^{x+y+q} \) such that \( d(z,C) = q^2 - 2 \). So the matrix \( G'^t \) generates a \([q^2 + q, 4, q^2 - 2] \) code. By Theorem 11, such a code does not exist. Hence \( R(C) = q^2 - 3 \). Since \( C \) is equivalent to \( C_{3,1}(q) \), \( R(C_{3,1}(q)) = q^3 - 3 \).

**THEOREM 13** :- \( R(C_{4,2}(q)) \leq q^3 - q - 2 \).

Proof:- Suppose \( R(C_{4,2}(q)) = q^3 - q - 1 \). Let \( x \in F_q^{x+y} \) with \( d(x,C_{4,2}(q)) = q^2(q-1) - 1 \). Then the matrix

\[
G = \left[ \begin{array}{cc} 1 & x \\ 0 & G_{4,2}(q) \end{array} \right]
\]

generates a \([q^2 + q^2 + 1, 5, q^2 - q] \) code \( C \). So \( \text{Res}(C,q^2 - q) \) is a \([q^2 + q + 1, 4, q^2 - 1] \) code. By Theorem 10, such a code does not exist. This proves the theorem.

By taking \( m = 4 \) and \( u = 2 \) in (7) and using Theorem 14, we have

**Corollary 14** \( R(C_{k,2}(q)) \leq q^{k-1} - q - 2 \).

**Corollary 15** \( 21 \leq R(C_{4,2}(3)) \leq 22 \).

Proof:- By Corollary 14, \( R(C_{4,2}(3)) \leq 22 \) and by (8), \( R(C_{4,2}(3)) \geq 21 \).

**THEOREM 16** :- \( R(S_4(3)) = 24 \), \( R(C_{4,1}(3)) = 23 \) and \( R(C_{k,1}(3)) \leq 3^{k-1} - 4 \) for \( k \geq 4 \).

Proof:- In [5], it is shown that \( R(S_4(3)) \leq 24 \). To see that \( R(S_4(3)) \geq 24 \), let \( A \) be a \([43,5,27] \) optimal ternary linear code with three equal coordinates \([13; \text{example 3}] \). Then \( A \) has a generator matrix of the form

\[
G_A = \left[ \begin{array}{ccc|c} 1 & 1 & 1 & x \\ 0 & 0 & 0 & G \end{array} \right]
\]

The matrix \( G \) generates a \([40,4,27] \) ternary code \( C \). Since \( d(x,C) = 24 \), \( R(S_4(3)) \geq 24 \).

Since \( C_{4,1}(3) \) is a punctured code of \( S_4(3) \), \( R(C_{4,1}(3)) \geq 23 \). If \( R(C_{4,1}(3)) = 24 \), then there exists a \( y \) such that \( d(y,C_{4,1}(3)) = 24 \). So the matrix

\[
G = \left[ \begin{array}{cc} 1 & 1 \\ 0 & y \end{array} \right]
\]

generates a \([41,5,26] \) ternary code, a contradiction to \( n_q(5, 26) = 42 \). Therefore \( R(C_{4,1}(3)) = 23 \). Hence by (8), \( R(C_{k,1}(3)) \leq 3^{k-1} - 4 \) for \( k \geq 4 \).

**References**


