VOL. 3, NO. 10, October 2013 ISSN 2225-7217
ARPN Journal of Science and Technology

http://www.ejournalofscience.org

Covering Radius of RM Binary Codes

[1] O.P.Vinocha, [2] J.S.Bhullar, [3] B.S.Brar
[1] Ferozepur College of Engineering and Technology, Ferozepur, Punjab, India
[2] Department of Applied Sciences, Malout Institute of Management and Information Technology (MIMIT), Malout, Punjab, India
[3] Department of Applied Sciences, Baba Farid College of Engineering and Technology, Bathinda, Punjab, India
[1] vinochar@yahoo.com, [2] bhullarjaskarn@rediffmail.com, [3] hodas.bfcet@yahoo.in

ABSTRACT

The strength and the covering radius of a binary self-complementary code are studied under different conditions. Some results for covering radius are found with different range of values of weight of code. We have generalized the results concerning relation between strength and covering radius of code. Then we have proved the result for binary code C of length n having strength s, which represents the relation among n, s, weight of codeword, and number of code words in code C. Further we have analyzed the particular results by using this relation for code C having strength more than 2, i.e. for strength s = 3, 4, 5, and obtained the range of values of covering radius. Lastly, we have analyzed the values of covering radius and found that in case of even suffix, the values are clear-cut fixed; but in case of odd suffix, only values of r_1, $r_{3\ are}$ fixed but afterwards the values become more and more scattered and problem of fixing unique value become more and more difficult.

Keywords: *Reed-Muller code, binary self-complementary code, cosset, weight, strength, covering radius, relation, generalization*

1. INTRODUCTION

The covering radius of a code $C \subseteq GF(2)^n$ is that it is the least integer r = r(C) such that each vector in $GF(2)^n$ is within Hamming distance r of some codeword in C. Delsarte (1973)[1] proved that r(C) is less than or equal to the external distance of C, where external distance of code C is the number of non-zero terms in the MacWilliams transform of distance distribution distribution of code C. Also, we define the covering radius of code C to be t = max.min.dist.(u,f), $f \in F^n, u \in C$. So, t is the true external distance ($s^{/}$) of code C, i.e. t is the maximum of the smallest weight in any cosset of C. Also, an (n, M, d = 2e + 1) code is perfect iff $s^{/}$ = e, e being the error-vector.(MacWilliams and Sloane(1977))[2]. Therefore, if a code C is an e-perfect code, then it is clear that r(C) = e. In particular, if a code C is one-error-correcting BCH code of length $n = 2^m - 1$, then t = 1, and hence code will have covering radius 1.

Gorenstein, Peterson and Zierler (1960)[3] proved that the two-error-correcting BCH code of length $2^m - 1$, has covering radius 3. Berger and Vander Horst (for $m \equiv 0 \pmod 4$)(1976)[4] Assmus and Mattson (1976)(for m odd)[5] and Helleseth(1978)(for $m \equiv 2 \pmod 4$))[6] proved that the three-error-correcting BCH code of length $2^m - 1$ has covering radius 5. Helleseth,T.; Klove, T. and Mykkeltvit, J(1978)[7] studied upper bounds on the covering radius of binary codes and classes of codes that attain these bounds.

2. RELATION BETWEEN STRENGTH AND COVERING RADIUS OF A CODE

A binary code has strength s, if each s-subset of the co-ordinates of the code, contains all binary s-tuples a constant number of times. Johannes J. Mykkeleit (1980)[8] defined that code C has strength s iff every subset of s columns of C is LI., i.e. if $C^{\perp}$ has no non-zero codewords of weight$\leq$ s. Also, if code C has strength s, then it also have strength $s^{/}$ for all integers $s^{/}$ such that $0 \leq s^{/} \leq s$.

Lemma 1:

Let C be a binary code of length n. Let $v \in GF(2)^n$. Then:

(i) If C has strength 1,then

$$\sum_{u \in v+C} w(u) = \frac{1}{2} n \,|\, C \,| \qquad (1)$$

(ii) If C has strength 2, then

$$\sum_{u \in v+C} w(u)^2 = \frac{1}{4}.n.(n+1) \,|\, C \,|, \qquad (2)$$

where |C|denotes the number of codewords in code C.

Theorem 1:

If code C is a binary code of length n and strength s = 1, then $r(C) \leq \left\lfloor \frac{n}{2} \right\rfloor$. (3)

Now before proceeding to Theorem 2, we have a definition as follows:

$1 = (1,1,1,\ldots,1) \in GF(2)^n$; $\bar{u}$ =1 + u for $\in GF(2)^n$

Theorem 2:

If C is a binary repetition code or a shortened Hadmard code of length n, which is (obtained from a normalized Hadmard matrix by deleting the first column and changing +1's to 0's and -1's to 1's), then

$$r(C) = \left\lfloor \frac{n}{2} \right\rfloor. \quad (4)$$

Now repetition code is self-complementary, and the shortened Hadamard code has strength 2, and in Theorem 2, one or the other condition holds, and we see that in relation to bound, there is no improvement in Theorem 2 as compared to the bound in Theorem 1. Therefore, by ensuring both these conditions simultaneously, we would like to analyse whether there is some improvement in the bound or not. In this light, we advance the discussion in the form of Theorem 3.

Theorem 3:

Let C be a binary self-complementary code of length n and strength s = 2.

(i) If w(u) = r, $w(\bar{u})$ = r, then: $r(C) = \left\lfloor \left(n - \sqrt{n}\right)/2 \right\rfloor$;

(ii) If w(u) > r, $w(\bar{u})$ < r, then the range of the values of ρ is:

$$\rho \in \left(-\infty, \frac{n - \sqrt{2n(1-n)}}{2} \right) \cup \left(\frac{n + \sqrt{2n(1-n)}}{2} \right)$$

and approximate value of ρ is: $\rho < \frac{(3n-2)}{4}$

$$where \;\; r = \frac{n}{2} - \rho, \; \rho \geq 0.$$

(iii) If w(u) < r, $w(\bar{u})$ > r, n >1, then the range of

$$\rho \in \left(-\infty, \frac{n - \sqrt{2n(1-n)}}{2} \right) \cup \left(\frac{n + \sqrt{2n(1-n)}}{2} \right)$$

the values of ρ is:

and approximate value of ρ is : $\rho < \frac{(3n-2)}{4}$

$$where \;\; r = \frac{n}{2} - \rho, \; \rho \geq 0.$$

(iv) If w(u) = r, $w(\bar{u})$ < r, then: $r(C) < \left\lfloor \left(n - \sqrt{n}\right)/2 \right\rfloor$

(v) If w(u) < r, $w(\bar{u})$ = r, then: $r(C) < \left\lfloor \left(n - \sqrt{n}\right)/2 \right\rfloor$

Proof:

Let $v \in GF(2)^n$ be a vector. Let distance of v to any codeword of code C is at least r,

i.e. let $w(u) \geq r$ for all $u \in v+C$ (5)

If $u = v + c \in v + C$, then $\bar{u} = v + \bar{c} \in v+C$ (because C is complementary, therefore if $c \in C$, then $\bar{c} = (c + 1) \in C$).

Also, $w(u) + w(\bar{u}) = n$ (6)

Moreover, if $w(u) \geq r$ for all $u \in v + C$, then $w(\bar{u}) \leq r$; and vice-versa. (7)

(i) Let w(u) = r, $w(\bar{u})$ = r.

Let us take $r = \frac{n}{2} - \rho, \; \rho \geq 0$ (8)

Now $w(u)^2 + w(\bar{u})^2 = w(u)^2 + (n - w(\bar{u}))^2$

(using(6))

$$= r^2 + (n-r)^2 = \left(\frac{n}{2} - \rho\right)^2 + \left(n - \left(\frac{n}{2} - \rho\right)\right)^2$$

(using(8))

$= (\frac{n}{2}-\rho)^2 + (\frac{n}{2}+\rho)^2 = 2.$

$[(\frac{n}{2})^2+\rho^2] = 2.[\frac{n^2}{4}+\rho^2]$

Therefore, $w(u)^2 + w(\bar{u})^2 = 2.[\frac{n^2}{4}+\rho^2]$ (9)

Because, the strength of code C is 2, therefore, applying Lemma 1(part(ii)), we have:

$$\sum_{u\in v+C} w(u)^2 = \frac{1}{4}n.(n+1)\,|C|$$

This implies:

$$\frac{1}{4}.n.(n+1).|C| = \left(\frac{1}{2}|C|\right).2\left(\frac{n^2}{4}+\rho^2\right) \quad (10)$$

(using(9) and using the fact that strength of code C is 2 which implies that contribution of each position in codeword of code C will be |C|/2, where |C| denotes the number of codewords in code C).

$$\Rightarrow \rho^2 = \frac{1}{4}.n \quad (11)$$

Now (8) is: $r = \frac{n}{2}-\rho,\ \rho \geq 0$

$= \frac{n}{2} - \left(\sqrt{\frac{1}{4}.n}\right)$ (using (11))

Therefore, $r = \frac{n-\sqrt{n}}{2}$ (12)

Because r, being covering radius of code C, is an integer, therefore, (12) implies that:

$r(C) = \lfloor (n-\sqrt{n})/2 \rfloor$.

(ii) Let $w(u) > r$, $w(\bar{u}) < r$,

Now $w(u)^2 + w(\bar{u})^2 < w(u)^2 + r^2$ (because $w(\bar{u}) < r$)

$< n^2 + r^2$ (because $w(u) + w(\bar{u}) = n$ implies that $w(u) < n$)

$= n^2 + (\frac{n}{2}-\rho)^2$ (using (8))

Therefore, $w(u)^2 + w(\bar{u})^2 = \frac{5n^2}{4} + \rho^2 - n\rho$ (13)

Because, the strength of code C is 2, therefore, applying Lemma 1(part(ii)), we have:

$$\sum_{u\in v+C} w(u)^2 = \frac{1}{4}n.(n+1)\,|C|$$

This implies:

$$\frac{1}{4}.n.(n+1).|C| < \left(\frac{1}{2}|C|\right).\left(\frac{5n^2}{4}+\rho^2-n\rho\right) \quad (14)$$

(using(13) and using the fact that strength of code C is 2 which implies that contribution of each position in codeword of code C will be |C|/2, where |C| denotes the number of codewords in code C).

$$\Rightarrow 4\rho^2 - 4n\rho + (3n^2-2n) > 0 \quad (15)$$

$\Rightarrow (2\rho-n)^2 > 2n-2n^2 \Rightarrow$

$|2\rho-n|^2 > 2n(1-n)$

$\Rightarrow |2\rho-n| > \sqrt{2n(1-n)}$

$$\Rightarrow \rho \in \left(-\infty, \frac{n-\sqrt{2n(1-n)}}{2}\right) \cup \left(\frac{n+\sqrt{2n(1-n)}}{2}\right) \quad (16)$$

This gives the range of the values of ρ.

Also, because ρ is very small, so ρ^2 will be so small, and it can be neglected. So, we get from (15) as:

$$-4n\rho + (3n^2-2n) > 0$$

$$\Rightarrow \rho < \frac{(3n-2)}{4} \quad (17)$$

This gives the approximate value of ρ.

Hence if $w(u) > r$, $w(\bar{u}) < r$, then the range of the values of ρ is:

$$\rho \in \left(-\infty, \frac{n-\sqrt{2n(1-n)}}{2}\right) \cup \left(\frac{n+\sqrt{2n(1-n)}}{2}\right)$$ and

approximate value of ρ is : $\rho < \frac{(3n-2)}{4}$.

(iii) Proceeding exactly as in part (ii) above, we can establish that if w(u) < r, w($\bar{u}$) > r, then the range of the values of ρ is:

$$\rho \in \left(-\infty, \frac{n-\sqrt{2n(1-n)}}{2}\right) \cup \left(\frac{n+\sqrt{2n(1-n)}}{2}\right)$$ and an

approximate value of ρ is : $\rho < \frac{(3n-2)}{4}$.

(iv) Now we discuss the case, when w(u)=r,w($\bar{u}$) < r.

Now $w(u)^2 + w(\bar{u})^2 = r^2 + w(\bar{u})^2$ (because w(u) = r)

$< r^2 + r^2$ (because w($\bar{u}$) < r)

$< r^2 + (n-r)^2$ (because r<(n-r))

$= (\frac{n}{2} - \rho)^2 + (n - (\frac{n}{2} - \rho))^2$ (using (8))

Therefore, $w(u)^2 + w(\bar{u})^2 < 2.[\frac{n^2}{4} + \rho^2]$ (18)

Because, the strength of code C is 2, therefore, applying Lemma 1(part(ii)), we have:

$$\sum_{u \in v+C} w(u)^2 = \frac{1}{4} n.(n+1) |C|$$

This implies:

$$\frac{1}{4}.n.(n+1).|C| = \left(\frac{1}{2}|C|\right).2\left(\frac{n^2}{4} + \rho^2\right)$$ (19)

(using(18) and using the fact that strength of code C is 2 which implies that contribution of each position in codeword of code C will be |C|/2, where |C| denotes the number of codewords in code C).

$$\Rightarrow \rho^2 > \frac{1}{4}.n$$ (20)

Now (8) is: $r = \frac{n}{2} - \rho,\ \rho \geq 0$

$$< \frac{n}{2} - \left(\sqrt{\frac{1}{4}.n}\right)$$ (using (20)

Therefore, $r < \frac{n-\sqrt{n}}{2}$ (21)

Because r, being covering radius of code C, is an integer,

Therefore, (21) implies that:

$r(C) = \lfloor (n - \sqrt{n})/2 \rfloor$.

(v) Proceeding exactly as in part (iv) above, we can analyse the case when w(u) < r, w($\bar{u}$) = r, and arrive at the conclusion that $r(C) < \lfloor (n - \sqrt{n})/2 \rfloor$

3. GENERALISATIONS OF THE RESULTS CONCERNING RELATION BETWEEN STRENGTH AND COVERING RADIUS OF A CODE

By Lemma 1, if C be a binary code of length n, and C has strength s = 1, and $v \in GF(2)^n$, then:

$$\sum_{u \in v+C} w(u) = \frac{1}{2}.n.|C|,$$ (22)

And if f C has strength s = 2, then

$$\sum_{u \in v+C} w(u)^2 = \frac{1}{4} n(n+1)|C| = \frac{1}{2^2} n(n+1)|C|$$ (23)

We discuss the generalization of above results in the form of following Theorem 4.

Theorem 4:

Let C be a binary code of length n. Let $v \in GF(2)^n$. If C has strength s,

then $\sum_{u \in v+C} \binom{w(u)}{s} = \frac{1}{2^s}.\binom{n}{s}.|C|$ (24)

Proof:

Clearly |v + C| = |C|, i.e. |C| and |v + C| will contain same number of codewords(vectors). Also strength of code C and strength of cosset v + C is the same. Therefore, v+C

will have strength s, iff C has strength s. This means that each s-subset of co-ordinates of code C and each s-subset of co-ordinates of cosset v + C will contain all binary s-tuples a constant number of times. So, it will be sufficient to prove the Theorem for v = 0.

If code C has strength s = 1, then each 1-subset of co-ordinates of code C will contain binary –tuples a constant number of tines. So, each position will have an equal number of zeros and ones. Hence each position will contribute |C| / 2 to the sum. If code C has strength s = 2, then each 2-subset of co-ordinates of code will contain binary 2-tuples a constant number of times. So, (1,1) will occur |C| / 4 or |C| / 2^2 times in two fixed positions. Arguing in this way, we will see that if code C has strength s, then (1,1,1,…..s times) will occur |C| / 2^s times in s fixed positions.

Because, length of code C is n, so each codeword in code C will have n positions, and number of ways of considering s fixed positions among n positions will be $\binom{n}{s}$. Therefore, weight of code C will be give by $\binom{n}{s} \times |C| / 2^s$. On the other hand, weight of code C will also be given by $\binom{\sum_{u \in v+C} w(u)}{s}$.As a result, we shall obtain:

$$\binom{\sum_{u \in v+C} w(u)}{s} = \binom{n}{s} \times |C| / 2^s$$

$$\text{i.e. } \binom{\sum_{u \in v+C} w(u)}{s} = \frac{1}{2^s} . \binom{n}{s} |C|$$

The result (24) of Theorem 4 leads to the results of Lemma 1, as shown below.

If code C has strength s=1, then result (24) will become as:

$$\sum_{u \in v+C} \binom{w(u)}{1} = \frac{1}{2^1} . \binom{n}{1} . |C|$$

$$\Rightarrow \sum_{u \in v+C} w(u) = \frac{1}{2} . n . |C|$$

which is the first result of Lemma 1, i.e. result (11).

If code C has strength s=2, then result (24) will become as:

$$\sum_{u \in v+C} \binom{w(u)}{2} = \frac{1}{2^2} . \binom{n}{2} . |C|$$

$$\Rightarrow \sum_{u \in v+C} \frac{(w(u)).(w(u)-1)}{2} = \frac{1}{4} . \frac{n.(n-1)}{2} . |C|$$

$$\Rightarrow \sum_{u \in v+C} w(u)^2 - \sum_{u \in v+C} w(u) = \frac{1}{4} . n . (n-1) . |C|$$

$$\Rightarrow \sum_{u \in v+C} w(u)^2 - \left(\frac{1}{2} . n . |C| \right) = \frac{1}{4} . n . (n-1) . |C|$$

(using result (1) of Lemma 1, part(i))

$$\Rightarrow \sum_{u \in v+C} w(u)^2 = \frac{1}{4} . n . (n+1) . |C| ,$$

which is the 2nd result of Lemma 1, i.e. the result (2).

Therefore, we see that result of Theorem 4, i.e. the result (24) leads to results (i) and (ii) of Lemma 1.This fact further strengthens the authenticity of Theorem 4. Now we can analyse the particular results by using result (24) of Theorem 4 for the code C having strength more than 2.

Let code C has strength 3, i.e. let s = 3. Therefore, we obtain from result (24) of Theorem 4, as :

$$\sum_{u \in v+C} \binom{w(u)}{3} = \frac{1}{2^3} . \binom{n}{3} . |C|$$

$$\Rightarrow \sum_{u \in v+C} \frac{(w(u))!}{3! . \{w(u)-3\}!} = \frac{1}{8} . \frac{n!}{3! . (n-3)} . |C|$$

$$\Rightarrow \sum_{u\in v+C} \frac{(w(u))....(w(u)-2)}{3!} = \frac{1}{8}.\frac{n(n-1)(n-2)}{3!}|C|$$

$$\Rightarrow \sum_{u\in v+C} w(u)^3 - 3\sum_{u\in v+C} w(u)^2 + 2\sum_{u\in v+C} w(u) = \frac{1}{8}.n.(n-1).(n-2).|C|.$$

$$\Rightarrow \sum_{u\in v+C} w(u)^3 - 3\left\{\frac{1}{4}n(n+1)|C|\right\} + 2\left\{\frac{1}{2}n|C|\right\} = \frac{1}{8}.n.(n-1).(n-2).|C|.$$

(using (1) and (2)

Therefore,

$$\sum_{u\in v+C} w(u)^3 = \frac{1}{8}(n^3+3n^2)|C| \quad (25)$$

Let code C has strength 4, i.e. let s = 4. Therefore, we obtain from result (24) of Theorem 4, as :

$$\sum_{u\in v+C} \binom{w(u)}{4} = \frac{1}{2^4}.\binom{n}{4}.|C|$$

$$\Rightarrow \sum_{u\in v+C} \frac{(w(u))\ldots\ldots\ldots(w(u)-3)}{4!} = \frac{1}{16}.\frac{n.(n-1).(n-2).(n-3)}{4!}.|C|.$$

$$\Rightarrow \sum_{u\in v+C} w(u)^4 - 6\sum_{u\in v+C} w(u)^3 + 11\sum_{u\in v+C} w(u)^2 - 6\sum_{u\in v+C} w(u) = \frac{1}{16}.n.(n-1).(n-2).(n-3).|C|.$$

$$\Rightarrow \sum_{u\in v+C} w(u)^4 - 6.\left\{\frac{1}{8}.(n^3+3n^2).|C|\right\} + 11\left\{\frac{1}{4}n.(n+1)|C|\right\} - 6\left\{\frac{1}{2}n.|C|\right\} = \frac{1}{8}.n.(n-1).(n-2).(n-3).|C|.$$

(using (1), (2) and (25)

Therefore:

$$\sum_{u\in v+C} w(u)^4 = \frac{1}{16}(n^4+6n^3+3n^2-2n)|C| \quad (26)$$

Let code C has strength 5, i.e. let s = 5. Therefore, we obtain from result (24) of Theorem 4, as :

$$\sum_{u\in v+C} \binom{w(u)}{5} = \frac{1}{2^5}.\binom{n}{5}.|C|$$

$$\Rightarrow \sum_{u\in v+C} \frac{(w(u))(w(u)-1)...(w(u)-4)}{5!} = \frac{1}{32}\frac{n(n-1)(n-2)(n-3)(n-4)}{5!}|C|$$

$$\Rightarrow \sum_{u\in v+C} w(u)^5 - 10.\sum_{u\in v+C} w(u)^4 + 35\sum_{u\in v+C} w(u)^3 - 50.\sum_{u\in v+C} w(u)^2 + 24.\sum_{u\in v+C} w(u) = \frac{1}{32}.n.(n-1).(n-2).(n-3).(n-4).|C|.$$

So,

$$\sum_{u\in v+C} w(u)^5 - 10\left\{\frac{1}{16}\left(n^4+6n^3+3n^2-2n\right)|C|\right\} + 35\left\{\frac{1}{8}n(n^2+3n)|C|\right\} - 50\left\{\frac{1}{4}n(n+1)|C|\right\} + 24\left(\frac{1}{2}n|C|\right) = \frac{1}{32}.n.(n-1).(n-2).(n-3).(n-4).|C|.$$

(using (1), (2), (25), and (26))

Therefore:

$$\sum_{u\in v+C} w(u)^5 = \frac{1}{32}\left(n^5+10n^4+15n^3-110n^2\right) \quad (27)$$

And so on. In this way, we can discuss the relation between weight of code C and its strength, and can have formulations for weight of code C in terms of length n of

code and number of codewords in the code, for various values of strength of code.

Now among the various cases in Theorem 3,we note that when w(u) = r,w($\bar{u}$) = r, then r(C) = $\lfloor (n-\sqrt{n})/2 \rfloor$;when w(u) = r, w($\bar{u}$)< r or when w(u) < r, w($\bar{u}$) = r, then r(C)< $\lfloor (n-\sqrt{n})/2 \rfloor$.

Combining these two cases, we have: r(C)≤ $\lfloor (n-\sqrt{n})/2 \rfloor$. In the process of proof of these cases, we come across formulations (10) and (19), and combining these, we obtain:

$$\sum_{u\in v+C} w(u)^2 = \frac{1}{4}.n.(n+1).|C| \le \left(\frac{1}{2}|C|\right).2\left(\frac{n^2}{4}+\rho^2\right)$$

$$or \sum_{u\in v+C} w(u)^2 \le \left(\frac{1}{2}|C|\right).\left[\left(\frac{n}{2}-\rho\right)^2+\left(\frac{n}{2}+\rho\right)^2\right],$$

The tentative generalization of this may be like this:

Theorem 5:

If code C is of strength s and is self-complementary, then:

$$\sum_{u\in v+C} w(u)^s \le \left(\frac{1}{2}|C|\right).\left[\left(\frac{n}{2}-\rho\right)^s+\left(\frac{n}{2}+\rho\right)^s\right] \quad (28)$$

If strength s of code C is 1, then (28) will become as:

$$\sum_{u\in v+C} w(u)^1 \le \left(\frac{1}{2}|C|\right).\left[\left(\frac{n}{2}-\rho\right)^1+\left(\frac{n}{2}+\rho\right)^1\right]$$

That is:

$$\sum_{u\in v+C} w(u) \le \frac{1}{2}.n.|C| \quad (29)$$

If strength s of code C is 2, then (28) will become as:

$$\sum_{u\in v+C} w(u)^2 \le \left(\frac{1}{2}|C|\right).\left[\left(\frac{n}{2}-\rho\right)^2+\left(\frac{n}{2}+\rho\right)^2\right]$$

$$\Rightarrow \sum_{u\in v+C} w(u)^2 \le \left(\frac{n^2}{4}+\rho^2\right).|C| \quad (30)$$

If strength s of code C is 3, then (28) will become as:

$$\sum_{u\in v+C} w(u)^3 \le \left(\frac{1}{2}|C|\right).\left[\left(\frac{n}{2}-\rho\right)^3+\left(\frac{n}{2}+\rho\right)^3\right]$$

$$\le \left(\frac{1}{2}|C|\right).\left[\left(\frac{n}{2}-\rho\right)^3+\left(\frac{n}{2}+\rho\right)^3\right]$$

$$\Rightarrow \frac{1}{8}\left(n^3+3n^2\right).|C|$$

$$\le \left(\frac{1}{2}|C|\right)\left[(n)\left(2\frac{n^2}{4}+2\rho^2-\frac{n^2}{4}+\rho^2\right)\right]$$

(using (25))

$$\Rightarrow \rho^2 \ge \frac{1}{4}n \qquad \Rightarrow (\frac{n}{2}-r)^2 \ge \frac{1}{4}n$$

$$(\because r=\frac{n}{2}-\rho,\ \rho\ge 0 \Rightarrow \rho=\frac{n}{2}-r)$$

$$\Rightarrow|\frac{n}{2}-r|^2\ge\frac{1}{4}n \qquad \Rightarrow|\frac{n}{2}-r|\ge\frac{\sqrt{n}}{2}$$

$$\Rightarrow r(C)\in\left(-\infty,\frac{n-\sqrt{n}}{2}\right] \cup\left[\frac{n+\sqrt{n}}{2},\infty\right)$$

Therefore, when code C is of strength s=3 and is self-complementary, then:

$$r(C)\in\left(-\infty,\frac{n-\sqrt{n}}{2}\right]\cup\left[\frac{n+\sqrt{n}}{2},\infty\right) \quad (31)$$

If strength s of code C is 4, then (28) will become as:

$$\sum_{u\in v+C} w(u)^4 \le \left(\frac{1}{2}|C|\right).\left[\left(\frac{n}{2}-\rho\right)^4+\left(\frac{n}{2}+\rho\right)^4\right]$$

$$\Rightarrow \frac{1}{16}(n^4+6n^3+3n^2-2n).|C| \le \left(\frac{1}{2}|C|\right).\left[\left(\left(\frac{n^2}{4}+\rho^2-n\rho\right)^2+\left(\frac{n^2}{4}+\rho^2 n\rho\right)^2\right).\right]$$

(using (26)

$$\Rightarrow 16\rho^4+24n^2\rho^2-(6n^3+3n^2-2n)\ge 0 \quad (32)$$

Now solve the equation:

$$16\rho^4+24n^2\rho^2-(6n^3+3n^2-2n)=0$$

$$\rho^2=\frac{(-3n^2)\pm\sqrt{9n^4+6n^3+3n^2-2n}}{4}$$

Now ρ^2 cannot be equal to $\frac{(-3n^2)-\sqrt{9n^4+6n^3+3n^2-2n}}{4}$, as ρ^2 is always positive. Therefore,

$$\rho^2=\frac{(-3n^2)+\sqrt{9n^4+6n^3+3n^2-2n}}{4}$$

$$Let\ \sqrt{9n^4+6n^3+3n^2-2n}-3n^2=\upsilon \quad (33)$$

$$\therefore \rho^2=\frac{\upsilon}{4}$$

$$Therefore,\ (32)\ implies:\ \rho^2\ge\frac{\upsilon}{4}$$

$$\Rightarrow\left(\frac{n}{2}-r\right)^2\ge\frac{\upsilon}{4}$$

$$(\because r=\frac{n}{2}-\rho,\ \rho\ge 0\Rightarrow\rho=\frac{n}{2}-r) \quad \Rightarrow\left|\frac{n}{2}-r\right|^2\ge\frac{\upsilon}{4}$$

$$\Rightarrow\left|\frac{n}{2}-r\right|\ge\frac{\sqrt{\upsilon}}{2}$$

$$\Rightarrow r(C)\in\left(-\infty,\frac{n-\sqrt{\upsilon}}{2}\right]\cup\left[\frac{n+\sqrt{\upsilon}}{2},\infty\right) \quad (34)$$

$$\therefore r(C)\le\frac{n-\sqrt{\upsilon}}{2} \quad (35)$$

$$Now\ (33)\ implies:\ n<\upsilon<n+1$$

$$Therefore,\ \upsilon>n\Rightarrow\sqrt{\upsilon}>\sqrt{n} \quad (36)$$

If n is not a perfect square, then: $\left\lfloor\frac{n-\sqrt{\upsilon}}{2}\right\rfloor=\left\lfloor\frac{n-\sqrt{n}}{2}\right\rfloor$. Therefore, (35) implies:

$$r(C)\le\left\lfloor\frac{n-\sqrt{n}}{2}\right\rfloor$$

If n is a perfect square, i.e. if $n = m^2$ (say), so that $\sqrt{\upsilon}>\sqrt{n}$ implies that $\sqrt{\upsilon}>m$, then:

$$\left\lfloor\frac{n-\sqrt{\upsilon}}{2}\right\rfloor=\left(\frac{m^2-m}{2}\right)-1$$

and therefore : $r(C)\le\left(\frac{m^2-m}{2}\right)-1$ (37)

If strength s of code C is 5, then (28) will become as:

$$\sum_{u\in v+C} w(u)^5 \le \left(\frac{1}{2}|C|\right).\left[\left(\frac{n}{2}-\rho\right)^5+\left(\frac{n}{2}+\rho\right)^5\right]$$

$$\Rightarrow \frac{1}{32}(n^5+10n^4+15n^3-110n^2)\,|C|$$
$$\leq \left(\frac{1}{2}|C|\right).$$
$$\left[\left(\left(\frac{n^2}{4}+\rho^2-n\rho\right)^2.\left(\frac{n}{2}-\rho\right)\right)+\left(\left(\frac{n^2}{4}+\rho^2 n\rho\right)^2.\left(\frac{n}{2}+\rho\right)\right)\right].$$

(using (27)

So,

$$16n\rho^4+8n^3\rho^2-(2n^4+3n^3-22n^2)\geq 0 \quad (38)$$

Now we solve the equation, which is quadratic in ρ^2:

$$16n\rho^4+8n^3\rho^2-(2n^4+3n^3-22n^2)=0$$

$$\therefore \rho^2=\frac{-(n^2)\pm\sqrt{n^4+2n^3+3n^2-22n}}{4}$$

Now ρ^2 cannot be equal to $\frac{-(n^2)-\sqrt{n^4+2n^3+3n^2-22n}}{4}$, as ρ^2 is always positive. Therefore,

$$\rho^2=\frac{-(n^2)+\sqrt{n^4+2n^3+3n^2-22n}}{4}$$

$$Let\ \sqrt{n^4+2n^3+3n^2-22n}-n^2=\mu \quad (39)$$

$$\therefore \rho^2=\frac{\mu}{4}$$

$$Therefore,\ (38)\ implies:\ \rho^2\geq\frac{\mu}{4}$$

$$\Rightarrow\left(\frac{n}{2}-r\right)^2\geq\frac{\mu}{4}$$

$$(\because r=\frac{n}{2}-\rho,\ \rho\geq 0\Rightarrow\rho=\frac{n}{2}-r)$$

$$\Rightarrow\left|\frac{n}{2}-r\right|^2\geq\frac{\mu}{4}\Rightarrow\left|\frac{n}{2}-r\right|\geq\frac{\sqrt{\mu}}{2}$$

$$\Rightarrow r(C)\in\left(-\infty,\frac{n-\sqrt{\mu}}{2}\right]\cup\left[\frac{n+\sqrt{\mu}}{2},\infty\right) \quad (40)$$

$$\therefore r(C)\leq\frac{n-\sqrt{\mu}}{2} \quad (41)$$

$$Now\ (39)\ implies: n<\mu<n+1$$

Therefore,

$$\mu>n \quad \Rightarrow\sqrt{\mu}>\sqrt{n} \quad (42)$$

If n is not a perfect square, then:

$$\left\lfloor\frac{n-\sqrt{\mu}}{2}\right\rfloor=\left\lfloor\frac{n-\sqrt{n}}{2}\right\rfloor$$

Therefore, (41) implies: $r(C)\leq\left\lfloor\frac{n-\sqrt{n}}{2}\right\rfloor$

If n is a perfect square, i.e. if $n = m^2$ (say), so that $\sqrt{\mu}>\sqrt{n}$ implies that $\sqrt{\mu}>m$, then:

$$\left\lfloor\frac{n-\sqrt{\mu}}{2}\right\rfloor=\left(\frac{m^2-m}{2}\right)-1$$ and

therefore: $r(C)\leq\left(\frac{m^2-m}{2}\right)-1$ (43)

So, we have the following Theorem:

Theorem 6:

Let C is a binary self-complementary code of length n, and of strength 4 or 5.

(i) If n is not a perfect square, then: $r(C)\leq\left\lfloor\frac{n-\sqrt{n}}{2}\right\rfloor$

(ii) If n is a perfect square, say, $n = m^2$ (say), then: $r(C)\leq\left(\frac{m^2-m}{2}\right)-1$

4. PROBLEM OF COVERING RADIUS WITH ODD SUFFIX

For $m \leq 5$, the cosset weight distribution of RM_m is known. We know that $r_0 = 0$, $r_1 = 0$, $r_2 = 1$, $r_3 = 2$, $r_4 = 6$, $r_5 = 12$. Now, we have a Theorem describing general formulation for r_m as follows:

Theorem 7:

For m ≥ 0, $r_m \geq 2^{m-1} - 2^{\lceil m/2 \rceil - 1}$

Now in Theorem 3, we see that when w(u)=r, w($\bar{u}$)=r, then r(C) = $\lfloor (n - \sqrt{n})/2 \rfloor$; when w(u) = r, w($\bar{u}$) < r, then r(C) < $\lfloor (n - \sqrt{n})/2 \rfloor$; when w(u) < r, w($\bar{u}$) = r, then r(C) < $\lfloor (n - \sqrt{n})/2 \rfloor$. Combining these, we see from Theorem 3 that if C is a binary self-complementary code of length n and strength and when w(u)=r, w($\bar{u}$)=r, or when w(u) = r, w($\bar{u}$) < r, or when w(u) < r, w($\bar{u}$) = r, then r(C) ≤ $\lfloor (n - \sqrt{n})/2 \rfloor$. By Theorem 8, we see that for m ≥ 0, $r_m \geq 2^{m-1} - 2^{\lceil m/2 \rceil - 1}$. Combining these two Theorems, we obtain:

$r_m \leq \lfloor (2^m - \sqrt{2^m})/2 \rfloor$ & $r_m \geq 2^{m-1} - 2^{\lceil m/2 \rceil - 1}$

(because in Theorem 3, length of code is n, therefore in r_m, n becomes as $n = 2^m$).

i.e. $r_{2m} \leq \lfloor (2^{2m} - \sqrt{2^{2m}})/2 \rfloor$

& $r_{2m} \geq 2^{2m-1} - 2^{\lceil 2m/2 \rceil - 1}$

i.e. $r_{2m} \leq \lfloor (2^{2m} - (2^{2m})^{1/2})/2 \rfloor$

& $r_{2m} \geq 2^{2m-1} - 2^{\lceil m \rceil - 1}$

i.e. $r_{2m} \leq \lfloor (2^{2m} - 2^m)/2 \rfloor$

& $r_{2m} \geq 2^{2m-1} - 2^{\lceil m \rceil - 1}$

i.e. $r_{2m} \leq \lfloor 2^{2m-1} - 2^{m-1} \rfloor$

& $r_{2m} \geq 2^{2m-1} - 2^{\lceil m \rceil - 1}$

i.e. $r_{2m} \leq 2^{2m-1} - 2^{m-1}$

& $r_{2m} \geq 2^{2m-1} - 2^{\lceil m \rceil - 1}$

(because r_{2m} is an integer)

i.e. $r_{2m} \leq 2^{2m-1} - 2^{m-1}$ (44)

Putting values of m=0,1,2,3,4,5,……., we obtain from (44): $r_0 = 2^{-1} - 2^{-1} = 0$, $r_2 = 2^1 - 2^0 = 2 - 1 = 1$, $r_4 = 2^3 - 2^1 = 8 - 2 = 6$, $r_6 = 2^5 - 2^2 = 32 - 4 = 28$, $r_8 = 2^7 - 2^3 = 128 - 8 = 120$, and so on.

Now it is obvious that:

$$\lfloor 2^{2m} - 2^{m-1}.\sqrt{2} \rfloor > 2^{2m} - 2^m \text{ for } m \geq 2. \quad (45)$$

By Theorem (3), we have: $r_m \leq \lfloor (2^m - \sqrt{2^m})/2 \rfloor$, and by Theorem (8), we have:

$$r_m \geq 2^{m-1} - 2^{\lceil m/2 \rceil - 1}.$$

Therefore, $r_{2m+1} \leq \lfloor (2^{2m+1} - \sqrt{2^{2m+1}})/2 \rfloor$,

$$r_{2m+1} \geq 2^{(2m+1)-1} - 2^{\left\lceil \frac{2m+1}{2} \right\rceil - 1}.$$

i.e. $r_{2m+1} \leq \left\lfloor 2^{2m} - 2^{\frac{2m+1}{2} - 1} \right\rfloor$,

$$r_{2m+1} \geq 2^{2m} - 2^{\left\lceil m + \frac{1}{2} \right\rceil - 1}.$$

i.e. $r_{2m+1} \leq \left\lfloor 2^{2m} - 2^{\frac{2m-1}{2}} \right\rfloor$,

$$r_{2m+1} \geq 2^{2m} - 2^{(m+1)-1}.$$

i.e. $r_{2m+1} \leq \left\lfloor 2^{2m} - 2^{m-\frac{1}{2}} \right\rfloor$,

$$r_{2m+1} \geq 2^{2m} - 2^m.$$

i.e. $r_{2m+1} \leq \lfloor 2^{2m} - 2^{m-1}.\sqrt{2} \rfloor$, $r_{2m+1} \geq 2^{2m} - 2^m$ for m ≥ 2. (46)

Therefore, from (45) & (46), we observe that because $\lfloor 2^{2m} - 2^{m-1}.\sqrt{2} \rfloor$ and $2^{2m} - 2^m$ are not equal for m ≥ 0, so we cannot combine these two results in (46) to obtain a single result for r_{2m+1}.

We obtain from (46):

Upper bound of r_{2m+1} is $\lfloor 2^{2m} - 2^{m-1}.\sqrt{2} \rfloor$, and Lower bound of r_{2m+1} *is* $2^{2m} - 2^m$ for m ≥ 2 (47)

Putting m = 2 in (47), we get:

Upper bound of $r_5 = \lfloor 2^4 - 2^{2-1}.\sqrt{2} \rfloor = \lfloor 16 - 2.(1.41) \rfloor = \lfloor 16 - 2.82 \rfloor = \lfloor 13.18 \rfloor = 13$; and Lower bound of $r_5 = 2^4 - 2^2 = 16 - 4 = 12$, which is the known value of r_5.

Putting m = 3 in (47), we get:

Upper bound of $r_7 = \lfloor 2^6 - 2^2.\sqrt{2} \rfloor = \lfloor 64 - 4.(1.41) \rfloor = \lfloor 64 - 5.64 \rfloor = \lfloor 58.36 \rfloor = 58$; and Lower bound of $r_7 = 2^6 - 2^3 = 64 - 8 = 56$.

Therefore, $56 \leq r_7 \leq 58$. Hence it is difficult to fix the value of r_7 as 56 or 57 or 58.

Putting m = 4 in (47), we get:

Upper bound of $r_9 = \lfloor 2^8 - 2^3.\sqrt{2} \rfloor = \lfloor 256 - 8.(1.41) \rfloor = \lfloor 256 - 11.28 \rfloor = \lfloor 244.72 \rfloor = 244$; and Lower bound of $r_9 = 2^8 - 2^4 = 256 - 16 = 240$.

Therefore, $240 \leq r_9 \leq 244$. Hence it is difficult to fix the value of r_9 as 140 or 241 or 242 or 243 or 244.

Putting m = 5 in (47), we get:

Upper bound of $r_{11} = \lfloor 2^{10} - 2^4.\sqrt{2} \rfloor = \lfloor 1024 - 16.(1.41) \rfloor = \lfloor 1024 - 22.56 \rfloor = \lfloor 1001.449 \rfloor = 1001$; and Lower bound of $r_{11} = 2^{10} - 2^5 = 1024 - 32 = 992$.

Therefore, $992 \leq r_{11} \leq 1001$. Hence it is difficult to fix the value of r_{11} as 992 or 993 or 994 or 995 or 996 or 997 or 998 or 999 or 1000 or 1001. And so on.

From this discussion, we conclude that in case of $r_0, r_2, r_4, r_6, \ldots\ldots$, the values are clear-cut fixed. But in case of $r_1, r_3, r_5, r_7, r_9, r_{11}, \ldots\ldots$, we observe that only values of r_1, r_3 are fixed(being 0 and 2 respectively), and after that in case of $r_5, r_7, r_9, r_{11}, \ldots\ldots$..the problem of fixing unique value of these become more and more difficult.

r_1=0.	r_0 = 0.
r_3 = 2.	r_2 = 1.
$12 \leq r_5 \leq 13$.	r_4 = 6.
$56 \leq r_7 \leq 58$.	r_6 = 28.
$240 \leq r_9 \leq 244$.	r_8 = 120.
$992 \leq r_{11} \leq 1001$.	r_{10} = 496.
……	…….
……	…….

So, in case of covering radius with even suffix, there is no problem of fixing the value. But in case of covering radius with odd suffix, the values of r_1, r_3 are fixed, but from r_5 onwards, the problem goes on becoming more and more difficult, we get more and more scattered values.

5. CONCLUSION

There is a close relation between strength and covering radius, and between covering radius and weight of a binary self-complementary code. For different ranges of weight of code, we have obtained different ranges of values of covering radius. The results concerning relation between strength and covering radius of code, can be generalized. The range of values of covering radius changes with the different values of strength of code. Also if strength of code is 4 or 5, then value of covering radius depends upon whether length of code is a perfect square or not. The values of covering radius with even suffix are fixed; but with odd suffix, in case of r_1 and r_3 the values are fixed, but afterwards the range of values become more and more scattered.

REFERENCES

[1] P. Delsarte (1973): "Four Fundamental Parameters of a Code and their Combinatorial Significance", Inform. Contr.,vol,23, pp. 407-438, 1973.

[2] MacWilliams, F.J. and Sloane, N.J.A.(1977): "The Theory of Error-Correcting Codes "Amsterdam: North Holland 1977.

[3] Gorenstein D., Peterson W., and Zierler N.(1960): "Two-Error Correcting Bose-Chaudhuri Codes are Quasi-Perfect", Inform. Contr,vol,3, pp. 291-294, 1960.

[4] Assmus Jr. E.F., and Mattson Jr. H.F. (1976): "Some Three-Error Correcting BCH Codes have Covering Radius 5", IEEE Trans. Inform. Theory, Vol. IT-22,pp.348-349, 1976.

[5] Berger T., and Vander Horst J.A. (1976): "Complete Decoding of Triple-Error Correcting Binary BCH Codes", IEEE Trans. Inform. Theory, Vol. IT-22,pp.138-147, 1976.

[6] Helleseth,T. (1978): "All Binary Three-Error-Correcting BCH Codes of Length 2^m -1 have Covering Radius 5", IEEE Tran. Inform. Theory, Vol. IT-24,pp. 257-258, 1978.

[7] Helleseth,T.; Klove, T.; Mykkeltvit, J(1978): "On the Covering Radius of Binary Codes", IEEE Transactions on Information Theory, Vol. IT-24,No. 5, pp.627-628, September,1978.

[8] Mykkeltvit, J(1980): "The Covering Radius of the (128,8) Reed-Muller Code is 56", IEEE Transactions on Information Theory, Vol. IT-26, No. 3, pp.359-362, May,1980.