Multicovering Bounds from Relative Covering Radii

Iiro Honkala*
Andrew Klapper†

Abstract

The multicovering radii of a code are a recently introduced natural generalizations of the covering radius measuring the smallest radius of balls around codewords that cover all m-tuples of vectors. In this paper we prove a new identity relating the multicovering radii of a code to a relativized notion of ordinary covering radius. This identity is used to prove new bounds on the multicovering radii of particular codes. [1]

Keywords: Covering radius, multicovering radius, coding theory, Hamming codes.
AMS Classification: 94B65 (94B75, 94B05, 05B40)
Running head: Multicovering Bounds from Relative Covering Radii

1 Introduction and Definitions

The concept of multicovering radius was introduced by Klapper [5] in the context of studying the existence of stream ciphers secure against a large class of attacks. Let C be a code of length n and m be a positive integer. The *m-covering radius of C* is the smallest integer r such that every set of m vectors in $\mathbf{F}^n$ is contained in at least one ball of radius r around a codeword in C.

*Department of Mathematics, University of Turku, 20014 Turku, Finland, honkala@utu.fi. Research supported by the Academy of Finland under grant 44002

†Dept. of Computer Science, 763H Anderson Hall, University of Kentucky, Lexington, KY, 40506-0046, klapper@cs.uky.edu. Project sponsored by the National Science Foundation under grant number NCR-9706078.

[1] The paper was presented in the IEEE International Symposium on Information Theory 2000, Sorrento, Italy.

We denote the m-covering radius of a code C by $R_m(C)$. Then $R(C) := R_1(C)$ is the covering radius of C. For results on the covering radius, we refer to the book by Cohen, Honkala, Litsyn and Lobstein [1]. For earlier results on multicovering radii, see [4, 5, 6].

In general we are interested in various extremal values associated with this notion:

$$
\begin{aligned}
t_m(n) &= R_m(\mathbf{F}^n) = \text{ the smallest } m\text{-covering radius among length } n \text{ codes.} \\
t_m(n,K) &= \text{ the smallest } m\text{-covering radius among } (n,K) \text{ codes, i.e., codes of} \\
&\quad\ \text{length } n \text{ with cardinality } K. \\
K_m(n,R) &= \text{ the smallest cardinality of a length } n \text{ code and } m\text{-covering radius } R. \\
\ell_m(a,R) &= \text{ the smallest length of a linear code with codimension } a \text{ and } m\text{-covering} \\
&\quad\ \text{radius } R.
\end{aligned}
$$

When $m = 1$ we sometimes omit the subscript m. As usual, when we are only concerned with linear codes, parentheses are replaced by square brackets and the size K is replaced by the dimension k. As with the classical covering radius, a variety of bounds are known for these quantities [5, 6], but precise values are only known in a few cases.

There are, of course, relationships among these values. These can be proved by straightforward generalizations of the arguments used by Cohen, et al. [1].

Lemma 1.1 *For positive integers m, n, R, a, k, and n_0 we have*

1. *If $\ell_m(a,R) \le n_0$ and $n \ge n_0$, then $t_m(n, 2^{n-a}) \le R$.*
2. *If $K_m(n,R) \le K \le 2^n$, then $t_m(n,K) \le R$.*
3. *If $K_m(n,R) > K$, then $t_m(n,K) > R$.*

The purpose of this paper is to derive new bounds by relating the multi-covering radii of a code to a relativized notion of covering radius. We obtain the following results: new upper bounds and, in some cases, precise values for $R_m(\mathbf{F}^n)$; precise values for $R_3(\mathcal{H}_r)$, where $\mathcal{H}_r$ is the Hamming code of degree r; lower bounds for $R_m(C)$ for certain values of m; and an upper bound on $R_m(C)$ in terms of the minimal distance of C.

For generality, we define the notion of relativized covering radius for multi-covering radii, although we only use the ordinary covering radius version in this paper.

Definition 1.2 *Let C and S be codes of length n, and let m be a positive integer. Then the m-*covering radius of S relative to C*, $R_m(S,C)$, is the smallest integer r such that for every $c^1, \cdots, c^m \in C$ there is an $x \in S$ such that $d(c^i, x) \le r$ for all $i = 1, \cdots, m$. We also let $t_m(s,C) = \min\{R_m(S,C) : |S| = s\}$.*

Note that $t_m(s, \mathbf{F}^n) = t_m(n, s)$.

2 A Fundamental Identity

In this section we prove a new identity relating the m-covering radius of a code C to the covering radii of cardinality m codes relative to C. For any code S, we denote the set of word-complements of elements of S by $\bar{S}$ (the complement of a word x is $x + 111\ldots1$ by definition).

Theorem 2.1 *Let C be a code of length n. Then*

$$R_m(C) = n - t_1(m, C).$$

Proof: Let S be any (n, m) code. Then

$$R_1(\bar{S}, C) \geq t_1(m, C), \tag{1}$$

with equality for at least one such S. Therefore there is some $c \in C$ such that for every $x \in \bar{S}$, $d(c, x) \geq t_1(m, C)$. This is the same as saying that there is some $c \in C$ such that for every $x \in S$, $d(c, x) \leq n - t_1(m, C)$. Since this holds for every (n, m) code S, we have $R_m(C) \leq n - t_1(m, C)$.

If equality holds in (1), then for every $c \in C$, there is an $x \in \bar{S}$ such that $d(c, x) \leq t_1(m, C)$. This is the same as saying that for every $c \in C$, there is an $x \in S$ such that $d(c, x) \geq n - t_1(m, C)$. Thus $R_m(C) \geq n - t_1(m, C)$. Since (1) holds for at least one S, we have $R_m(C) = n - t_1(m, C)$. □

For $C = \mathbf{F}^n$ we obtain the following corollary, which is essentially a restatement of Theorem 19.4.4 of Cohen, et. al. [1] (cf. also Theorem 19.4.2).

Corollary 2.2 *For all natural numbers $n, m \geq 1$, $t_m(n) = R_m(\mathbf{F}^n) = n - t_1(n, m)$.*

Proof: This follows from Theorem 2.1 with $C = \mathbf{F}^n$ and the fact that $t_1(m, \mathbf{F}^n) = t_1(n, m)$. □

Thus bounds on $t_1(n, m)$ give bounds on $R_m(\mathbf{F}^n)$. It was previously shown [5] that

$$R_m(\mathbf{F}^n) \geq \frac{n + \lfloor \log_2(m) \rfloor - 1}{2} \tag{2}$$

for all $m \leq 2^n$. Since $t_1[n, k] \geq t_1(n, 2^k)$, an upper bound on $t_1(n, m)$ or $t_1[n, k]$ also gives us a lower bound on $R_m(C)$ for any length n code C. Furthermore, by Lemma 1.1, a bound of the form $\ell_1(a, R) = \ell(a, R) \leq n_0$ gives a bound $R_{2^{n-a}}(C) \geq n - R$ for any $n \geq n_0$ and any C of length n. Similarly, $K_1(n, R) \leq k$ if and only if $R_k(C) \geq n - R$

k	$t[n,k]$	$R_{2^k}(C) \geq$	if
1	$\left\lfloor \frac{n}{2} \right\rfloor$	$\left\lceil \frac{n}{2} \right\rceil$	$n \geq 1$
2	$\left\lfloor \frac{n-1}{2} \right\rfloor$	$\left\lceil \frac{n+1}{2} \right\rceil$	$n \geq 2$
3	$\left\lfloor \frac{n-2}{2} \right\rfloor$	$\left\lceil \frac{n+2}{2} \right\rceil$	$n \geq 3$
4	$\left\lfloor \frac{n-4}{2} \right\rfloor$	$\left\lceil \frac{n+4}{2} \right\rceil$	$n \geq 4$, $n \neq 5$
5	$\left\lfloor \frac{n-5}{2} \right\rfloor$	$\left\lceil \frac{n+5}{2} \right\rceil$	$n \geq 5$, $n \neq 6$
6	$\leq \left\lfloor \frac{n-8}{2} \right\rfloor$	$\left\lceil \frac{n+8}{2} \right\rceil$	$n \geq 14$
7	$\leq \left\lfloor \frac{n-9}{2} \right\rfloor$	$\left\lceil \frac{n+9}{2} \right\rceil$	$n \geq 19$
8	$\leq \left\lfloor \frac{n-16}{2} \right\rfloor$	$\left\lceil \frac{n+16}{2} \right\rceil$	$n \geq 127$
$2p+1$	$\leq \left\lfloor \frac{n-2^p}{2} \right\rfloor$	$\left\lceil \frac{n+2^p}{2} \right\rceil$	$n \geq 2^{2p}-1$
$2p$	$\leq \left\lfloor \frac{n-2^{p-1/2}}{2} \right\rfloor$	$\left\lceil \frac{n+2^{p-1/2}}{2} \right\rceil$	$n \geq 2^{2p-1}$

Table 1: Lower bounds on $R_{2^k}(C)$ for small k.

for every code of length n. Many such bounds are known, and they are well surveyed by Cohen, et al. [1]. We summarize the implications for the m-covering radius of $\mathbf{F}^n$ in several tables. Table 1 is a corollary of Cohen et al.'s Theorems 5.2.3, 5.2.7, 5.2.10, 5.2.16, and 5.2.21. Here C is any code of length n. We also have $t_1[5,4] = t_1[6,5] = 1$, so $R_{16}(C) \geq 4$ if C has length 5, and $R_{32}(C) \geq 5$ if C has length 6. The first three lines of the table actually follow from equation (2). In fact, this earlier result gives equality in these cases.

Another set of bounds arises from bounds on $\ell(a,b)$. Table 2 arises from Theorems 5.3.7, 5.4.27, 5.4.28, and 5.4.29 of Cohen et al.'s book [1].

$n \geq$	$m \geq$	a	$R_{2^a}(C) \geq$
$2^{2m+1} - 2^m - 1$	1	$n - 4m$	$n - 2$
$2^{2m+1} + 2^{2m} - 2^m - 2$	2	$n - 4m - 1$	$n - 2$
$2^{2m+2} - 2^m - 2$	2	$n - 4m - 2$	$n - 2$
$2^{2m+2} + 2^{2m+1} - 2^m - 2$	2	$n - 4m - 3$	$n - 2$
$27 \cdot 2^{m-4} - 1$	4	$n - 2m$	$n - 2$
$5 \cdot 2^{m-1} - 1$	1	$n - 2m - 1$	$n - 2$
$155 \cdot 2^{m-6} - 2$	6	$n - 3m$	$n - 3$
$152 \cdot 2^{m-6} - 1$	9	$n - 3m$	$n - 3$
$3 \cdot 2^m - 1$	7	$n - 3m - 1$	$n - 3$
$1024 \cdot 2^{m-8} - 1$	4	$n - 3m - 2$	$n - 3$
$822 \cdot 2^{m-8} - 2$	8	$n - 3m - 2$	$n - 3$
$821 \cdot 2^{m-8} - 1$	13	$n - 3m - 2$	$n - 3$
$47 \cdot 2^{m-4} - 1$	11	$n - 4m$	$n - 4$
$896 \cdot 2^{m-8} - 2$	8	$n - 4m - 1$	$n - 4$
$896 \cdot 2^{m-8} - 3$	10	$n - 4m - 1$	$n - 4$
$895 \cdot 2^{m-8} - 1$	15	$n - 4m - 1$	$n - 4$
$992 \cdot 2^{m-8} - 2$	8	$n - 4m - 2$	$n - 4$
$992 \cdot 2^{m-8} - 3$	10	$n - 4m - 2$	$n - 4$
$991 \cdot 2^{m-8} - 1$	15	$n - 4m - 2$	$n - 4$
$1248 \cdot 2^{m-8} - 3$	10	$n - 4m - 3$	$n - 4$
$1247 \cdot 2^{m-8} - 1$	15	$n - 4m - 3$	$n - 4$

Table 2: Lower bounds on $R_{2^a}(C)$ for large a.

3 Corollaries

It is known from Klapper [5] that for all $n \geq 3$

$$R_2(\mathbf{F}^n) = R_3(\mathbf{F}^n) = \left\lceil \frac{1}{2}n \right\rceil$$

and

$$R_4(\mathbf{F}^n) = R_5(\mathbf{F}^n) = \left\lceil \frac{1}{2}(n+1) \right\rceil.$$

Using Corollary 2.2 and the known results about $K(n, R)$, the minimum cardinality of a binary code of length n and covering radius R, we can determine $R_6(\mathbf{F}^n)$ and $R_7(\mathbf{F}^n)$.

Theorem 3.1 *For all $n \geq 4$ we have*

$$R_6(\mathbf{F}^n) = \left\lceil \frac{1}{2}(n+1) \right\rceil$$

and

$$R_7(\mathbf{F}^n) = \left\lceil \frac{1}{2}(n+2) \right\rceil.$$

Proof: We know — see Cohen, Lobstein and Sloane [2] and Honkala [3] — that $K(2R+2, R) = 4$ for all $R \geq 1$, $K(2R+3, R) = 7$ for all $R \geq 1$ and $K(2R+4, R) \geq 8$ for all $R \geq 0$.

By Lemma 1.1 this implies that $t_1(n, 6) = \frac{1}{2}(n-1)$ for odd $n \geq 5$ and $t_1(n, 6) = \frac{1}{2}(n-2)$ for even $n \geq 4$. Hence $t_1(n, 6) = \left\lfloor \frac{1}{2}(n-1) \right\rfloor$ and, by Corollary 2.2,

$$R_6(\mathbf{F}^n) = n - t_1(n, 6) = \left\lceil \frac{1}{2}(n+1) \right\rceil.$$

Similarly, $t_1(n, 7) = \frac{1}{2}(n-3)$ for all odd $n \geq 5$ and $t_1(n, 7) = \frac{1}{2}(n-2)$ for even $n \geq 4$. Hence $t_1(n, 7) = \left\lfloor \frac{1}{2}(n-2) \right\rfloor$ and, by Corollary 2.2,

$$R_7(\mathbf{F}^n) = n - t_1(n, 7) = \left\lceil \frac{1}{2}(n+2) \right\rceil.$$

□

Using Corollary 2.2 and the results in Section 12.5 of Cohen, et. al. [1] we obtain asymptotic results on $R_m(\mathbf{F}^n)$. For instance, using Theorems 12.5.1 (sphere-covering bound) and 12.5.10. (from Lovász, Spencer and Vesztergombi [7]) we obtain the following two theorems.

Theorem 3.2 *For all n and m,*

$$R_m(\mathbf{F}^n) \leq \frac{1}{2}n + \sqrt{n \log_2 m \ln 2/2}.$$

Theorem 3.3 *For all n and m,*

$$R_m(\mathbf{F}^n) \leq \frac{1}{2}n + 12\sqrt{m}.$$

4 On the 3-covering radius of Hamming codes

Let $\mathcal{H}_r$ denote the Hamming code of order r. It was shown by Klapper [5] that for any $m \geq 2$ and $r \geq 2$,

$$2^{r-1} \leq R_m(\mathcal{H}_r) \leq 2^{r-1} + c_m,$$

where c_m is a constant depending only on m. It was also shown that $R_m(\mathcal{H}_2) = 3$ for $m \geq 2$; for $r \geq 3$ we have $R_2(\mathcal{H}_r) = 2^{r-1}$; and for $m = 3, 4, 5$ we have

$$2^{r-1} \leq R_m(\mathcal{H}_r) \leq 2^{r-1} + 1.$$

However, in this last case the precise value was unknown. In this section, using Theorem 2.1, we determine exactly the 3-covering radius of the Hamming codes. The proof is based on the following lemma.

Lemma 4.1 *A binary code of odd length n, cardinality three and covering radius $\frac{1}{2}(n-1)$ contains a word-complement pair.*

Proof: Step 1: We first show that the covering radius of the code consisting of the three codewords

$$\begin{array}{cccc} c_1 & 11\ldots1 & 00\ldots0 & 00\ldots0 \\ c_2 & 00\ldots0 & 11\ldots1 & 00\ldots0 \\ c_3 & \underbrace{00\ldots0}_{\alpha} & \underbrace{00\ldots0}_{\beta} & \underbrace{11\ldots1}_{\gamma} \end{array}$$

where $\alpha \leq \beta \leq \gamma$ equals

$$t = \alpha + \left\lfloor \frac{\beta+\gamma}{2} \right\rfloor.$$

For every $x \in \mathbf{F}^n$ we have $d(x, C) \leq \left\lfloor \frac{1}{2}(d(x, c_2) + d(x, c_3)) \right\rfloor \leq t$. On the other hand, take $x \in \mathbf{F}^n$ which has α ones in the beginning, then $\left\lceil \frac{1}{2}(\alpha+\beta) \right\rceil$ ones among the next β and $\left\lceil \frac{1}{2}(\alpha+\gamma) \right\rceil$ ones among the last γ coordinates. Then

$$d(x, c_1) = \left\lceil \frac{1}{2}(\alpha+\beta) \right\rceil + \left\lceil \frac{1}{2}(\alpha+\gamma) \right\rceil,$$

$$d(x, c_2) = \alpha + \left(\beta - \left\lceil \frac{1}{2}(\alpha+\beta) \right\rceil\right) + \left\lceil \frac{1}{2}(\alpha+\gamma) \right\rceil = \left\lfloor \frac{1}{2}(\alpha+\beta) \right\rfloor + \left\lceil \frac{1}{2}(\alpha+\gamma) \right\rceil,$$

and

$$d(x, c_3) = \alpha + \left\lceil \frac{1}{2}(\alpha+\beta) \right\rceil + \left(\gamma - \left\lceil \frac{1}{2}(\alpha+\gamma) \right\rceil\right) = \left\lceil \frac{1}{2}(\alpha+\beta) \right\rceil + \left\lfloor \frac{1}{2}(\alpha+\gamma) \right\rfloor.$$

Because $d(x, c_1) \geq d(x, c_2)$, it suffices to show that $d(x, c_2) \geq t$ and $d(x, c_3) \geq t$. If β and γ have the same parity, then $d(x, c_2)$ and $d(x, c_3)$ both equal t. If β and γ have different parities, then $t = \alpha + \frac{1}{2}(\beta + \gamma - 1)$, and exactly one of $d(x, c_2)$ and $d(x, c_3)$ equals t and the other $t + 1$. Hence $d(x, C) = t$, proving that C has covering radius t.

Step 2: Assume now that we have a code of odd length n with three codewords and covering radius $\frac{1}{2}(n-1)$. By taking a suitable translate if necessary we may assume that in each coordinate all codewords have 0's or at most one of the codewords has 1. Assume that the number of identically zero coordinates is i, and that by puncturing these i coordinates we obtain the code C in Step 1 of length $n - i$. By Step 1, the covering radius of our original code equals

$$s = i + \alpha + \left\lfloor \frac{1}{2}(\beta + \gamma) \right\rfloor$$

and in particular

$$s \geq i + \left\lfloor \frac{1}{2}(n - i) \right\rfloor > \frac{1}{2}(n - 1)$$

if $i > 0$. Hence $i = 0$ and

$$s = \left\lfloor \frac{1}{2}(n + \alpha) \right\rfloor > \frac{1}{2}(n - 1)$$

unless $\alpha = 0$. Hence $\alpha = 0$, and c_2 is the complement of c_3. $\square$

Theorem 4.2 $t_1(3, \mathcal{H}_r) = \frac{1}{2}(n-1) = 2^{r-1} - 1$ *for all* $r \geq 3$.

Proof: Assume that C consists of three codewords c_1, c_2, and c_3 of length $n = 2^r - 1$ such that the balls of radius $\frac{1}{2}(n-3) = 2^{r-1} - 2$ centered at the codewords of C contain all the codewords of the Hamming code $\mathcal{H}_r$. Because the covering radius of the Hamming code is one, this implies that the balls of radius $2^{r-1} - 1$ centered at the words c_1, c_2 and c_3 cover the whole space $\mathbf{F}^n$. By the previous lemma this is only possible if the set $\{c_1, c_2, c_3\}$ contains a word-complement pair: say, c_2 is the complement of c_3. But we know that $R_2(\mathcal{H}_r) = \frac{1}{2}(n+1) = 2^{r-1}$ for $r \geq 3$ and that there is a codeword $c \in \mathcal{H}_r$ such that $d(c, c_2), d(c, c_3) \in \{\frac{1}{2}(n-1), \frac{1}{2}(n+1)\}$. The Hamming code is self-complementary, and therefore also $\overline{c} \in \mathcal{H}_r$. Neither c nor $\overline{c}$ is contained in the spheres $B_{(n-3)/2}(c_2)$ and $B_{(n-3)/2}(c_3)$. Since their mutual distance is n, they cannot both belong to $B_{(n-3)/2}(c_1)$, either. This contradiction proves that $t_1(3, \mathcal{H}_r) \geq \frac{1}{2}(n-1)$. The opposite inequality is clear. $\square$

Theorem 4.3 $R_3(\mathcal{H}_r) = \frac{1}{2}(n+1) = 2^{r-1}$ *for all* $r \geq 3$.

5 A Sphere Bound

Theorem 5.1 *Suppose C is a code with length n, and $m < |C|$. Then*

$$R_m(C) \leq n - \frac{1}{2}d_0,$$

where d_0 is the largest minimum distance among the $(m+1)$-element subcodes of C. In particular, if the minimum distance of C is d, then $R_m(C) \leq n - \frac{1}{2}d$.

Proof: By Theorem 2.1 it suffices to prove that $t_1(m, C) \geq \frac{1}{2}d_0$. If not, $t_1(m, C) < \frac{1}{2}d_0$, which is impossible because we know that C has an $(m+1)$-element subcode C_0 with minimum distance d_0 and therefore no ball $B_t(x)$ with $t < \frac{1}{2}d_0$ can cover more than one element of C_0. □

References

[1] G. Cohen, I. Honkala, S. Litsyn, A. Lobstein: Covering Codes, Elsevier, Amsterdam, 1997.

[2] G. D. Cohen, A. C. Lobstein, N. J. A. Sloane, Further results on the covering radius of codes, IEEE Trans. Inform. Theory, 32(1986), pp. 680–694.

[3] I. S. Honkala, Modified bounds for covering codes, IEEE Trans. Inform. Theory, 37(1991), pp. 351–365.

[4] I. Honkala, A. Klapper, Bounds for the multicovering radii of Reed-Muller codes with applications to stream ciphers, Designs, Codes, and Cryptography, to appear.

[5] A. Klapper, The Multicovering radii of codes, IEEE Trans. Info. Theory, 43(1997), pp. 1372–1377.

[6] A. Klapper, Improved lower bounds for multicovering codes, IEEE Trans. Inform. Theory, to appear.

[7] L. Lovász, J. H. Spencer, K. Vesztergombi, Discrepancy of set-systems and matrices, European J. Combinatorics, 7(1986), pp. 151–160.