The Multicovering Radii of Codes
Preliminary Version

Andrew Klapper*

May 23, 1996

Abstract

The covering radius of a code is the least r such that the set of balls of radius r around codewords covers the entire ambient space. We introduce a generalization of the notion of covering radius. The *m-covering radius* of a code is the least radius such that the set of balls of the radius covers all m-tuples of elements in the ambient space. We investigate basic properties of m-covering radii. We investigate whether codes exist with given m-covering radii (they don't always). We derive bounds on the size of the smallest code with a given m-covering radius, based on generalizations of the sphere bound and the method of counting excesses.

1 Introduction – Basic Concepts

The *covering radius* of a block code C is the smallest radius such that the set of balls of that radius covers the ambient space. More precisely, if C has length n, it is the smallest integer t such that every vector of length n has distance at most t from at least one code word. This concept has been the subject of hundreds of papers in the past couple of decades. See [2] for a comprehensive survey and thorough bibliography on the subject. In this paper we investigate simultaneous coverings of m-tuples of vectors, rather than single vectors. The *m-covering radius* of C is the smallest radius such that every m-tuple of vectors in the ambient space is contained in at least one ball of that radius around

*Dept. of Computer Science, 763H Anderson Hall, University of Kentucky, Lexington, KY, 40506-0046, klapper@cs.engr.uky.edu. Project sponsored by the National Science Foundation under grant number NCR-9400762.

some codeword. More precisely, if m is a positive integer, then the m-covering radius $t_m(C)$ of a code C of length n is the smallest integer t such that for every collection S of m vectors of length n, there is a code word v in C whose distance from every u in S is at most t. Thus for $m = 1$ we have the ordinary covering radius of C. At times we will also refer to $t_m(C)$ as a *multicovering radius* of C. In this paper we study the basic properties of multicovering radii and prove basic bounds on the existence of codes with certain parameters related to multi-covering radii.

The basic questions concerning multicovering radii concern bounds on certain code parameters given others. For given length, m, and t, what is the smallest length n code with $t_m = t$? What if we constrain the minimum distance or require that C be maximum or maximal? As with ordinary covering radius, precise general answers to these questions are unlikely. Thus we concentrate on finding upper and lower bounds, and in exploring relationships among the answers for different sets of parameters. The notion of multicovering radius makes sense over any alphabet, however, in this paper we restrict our attention to binary codes.

The notion of multicovering radius arose from investigations concerning the cryptanalysis of stream ciphers. Recall that a stream cipher is determined by a binary sequence B that is XORed with the message. In various cryptanalytic attacks, an algorithm is used to determine an efficient generator for B given a small number of bits of B [7, 3, 5]. We have recently investigated whether there exist efficient generators of sequences that resist all possible attacks of this general type [4]. (The answer is yes, but the results give no help in finding an efficient construction for such a family of sequences.) More generally, we consider attacks in which the attacker only hopes to correctly generate a substantial fraction of the bits of B. Using properties of the covering radius of Reed-Muller codes, we show that there exists an efficiently generated family of sequences that is secure against all such attacks in the sense that, for each such attack, there are infinitely many sequences in the family that resist the attack. A better result would be that the family resists all such attacks in the sense that, for each such attack, all but finitely many of the sequences resists the attack. Extending the techniques used seems to depend on finding good bounds for the multi-covering radii of efficiently generated codes. The idea is to show that for any set S of m sequences, there is an efficiently generated sequence B that is far from all the sequences in S. This is equivalent to saying that the complement of B is close to every sequence in S, hence is a statement that an m-covering radius is small. Beyond these questions, multi-covering radii are interesting in their own right as natural generalizations of the covering radius.

In Section 2 we establish notation. In Section 3 we consider what happens to multicovering radii under various constructions – changes in parameters, Cartesian product, the $(u, u+v)$ construction, repetition, and lengthening by the addition of a parity check. In Section 4 we prove various lower bounds, including generalizations of the sphere bound and the method of counting excesses. In Section 5 we find the sizes of the smallest codes that m-cover $\mathbf{F}^n$ with large radius. Finally, in Section 6 we consider the multicovering radii of repetition and Hamming codes.

2 Notation and Terminology

As much as possible, we have attempted to make our notation consistent with that used by Cohen, Litsyn, Lobstein and Mattson in their recent survey paper [2]. Thus we have

$\mathbf{N}$ = the set of natural numbers; $\mathbf{N}^* = \mathbf{N}$
$\{0\}$.

$\mathbf{F} = GF(2) = \{0, 1\}$.

For $x \in \mathbf{F}^n$, $\text{supp}(x) = \{i : x_i \neq 0\}$. The complement of x is denoted x' ($x'_i = 1 - x_i$).

$\text{wt}(x) = |x| = |\text{supp}(x)|$, the Hamming weight of x. The weight of a set S is the maximum of the weights of its elements, $\text{wt}(S) = \max\{\text{wt}(x : x \in S\}$.

For $x, y \in \mathbf{F}^n$, $d(x, y) = \text{wt}(x+y)$, the distance between x and y. This is the number of coordinate locations in which x and y differ. If S is a set, $d(x, S) = \min\{d(x, y) : y \in S\}$. The covering radius of x for S is $cov(x, S) = \max\{d(x, y) : y \in S\}$, the size of the smallest ball centered at x that contains all of S. If C is a code, the covering radius of C for S is $cov(C, S) = \min\{cov(c, S) : c \in C\}$, the size of the smallest ball centered at some x in C that contains all of S. Thus the covering radius of C is $\max\{cov(C, S) : |S| = m\}$.

$(u|v)$ is the concatenation of x and y.

$1^n, 0^n$ are the all 1 and all 0 vectors of length n.

For $x \in \mathbf{F}^n$, $B_t(x) = \{y \in \mathbf{F}^n : d(x, y) \leq t\}$, and $V(n, t) = |B_n(t)|$.

A set C (m, t)-*covers* (or simply covers if there is no ambiguity) a set V if for all $x^1, \cdots, x^m \in V$, there is a $c \in C$ such that $\forall i = 1, \cdots, m : d(x^i, c) \leq t$. Such a C is called an (m, t)-covering of V.

$t_m(C)$ = m-covering radius of C.

$\dim(C)$ = dimension of a linear code C.

$d(C)$ = minimum distance of code C.

$[n, k, d]_m t$ = binary linear code of length n, dimension k, minimum distance d, and m-covering radius t.

$(n, K)_m t$ = binary code of length n, cardinality K, and m-covering radius t.

$t_m[n, k]$ = smallest m-covering radius among all $[n, k]$ codes.

$t_m(n, k)$ = smallest m-covering radius among all (n, k) codes.

$k_m[n,t]$ = smallest dimension of a binary linear code of length n and m-covering radius t.

$K_m(n,t)$ = smallest cardinality of a binary code of length n and m-covering radius t.

$\binom{a}{b} = 0$ if $b < 0$ or $b > a$.

2.1 The Translate Leader

If C is a code, $c \in C$, and $S = (v_1, \cdots, v_m)$ is a set of vectors, then $cov(C,S) = cov(C, S+c)$, where $S + c = \{x + c : x \in S\}$. A *translate* of C is a set of m-tuples, $S +_m C = \{S + c : c \in C\}$, and a *translate leader* is an m-tuple $T \in S +_m C$ such that $\mathrm{wt}(T)$ is minimal. The m-covering radius of C is the weight of the maximal weight translate leader.

3 Basic Relationships

Certain basic relations hold as we vary the parameters for covering radii. The proofs are straightforward.

Proposition 3.1 *1. If $C_1 \subseteq C_2$, then $t_m(C_1) \geq t_m(C_2)$.*

2. For any code C and $m \in \mathbf{N}^*$, $t_m(C) \leq t_{m+1}(C)$.

3. For any $n, m, k \in \mathbf{N}^*$, $t_m(n,k) \leq t_{m+1}(n,k)$ and $t_m[n,k] \leq t_{m+1}[n,k]$.

4. For any $n, m, k \in \mathbf{N}^*$, $t_m(n,k) \geq t_m(n,k+1)$ and $t_m[n,k] \geq t_m[n,k+1]$.

5. For any $n, m, t \in \mathbf{N}^*$, $K_m(n,t) \leq K_{m+1}(n,t)$ and $k_m[n,t] \leq k_{m+1}[n,t]$.

6. For any $n, m, t \in \mathbf{N}^*$, $K_m(n,t) \geq K_m(n,t+1)$ and $k_m[n,t] \geq k_m[n,t+1]$.

We next consider the relationship between the multicovering radii of two codes and various codes that can be built from them. For $i = 1, 2$, let C_i be an $[n_i, k_i, d_i]$ code.

3.1 Cartesian Product

Let $C = C_1 \times C_2 = \{(x|y) : x \in C_1, y \in C_2\}$. This code has type $[n_1 + n_2, k_1 + k_2, \min d_1, d_2]$. If S is a set of m vectors in $\mathbf{F}^{n_1+n_2}$, then the sets of projections on the first and second components are within $t_m(C_1)$ and $t_m(C_2)$ of some code words in C_1 and C_2, respectively. Thus

$$t_m(C) \leq t_m(C_1) + t_m(C_2). \tag{1}$$

When $m = 1$ this inequality becomes an equality. However, for $m \geq 2$, it may be strict. For example, if $C_1 = C_2 = \{(0,0),(0,1)\}$, then $t_2(C_i) = 2$, while $t_2(C_1 \times C_2) = 3$.

On the other hand, suppose S_i is a set of m_i vectors of length n_i whose distance to C_i equals a_i $(i = 1,2)$. Let $S = \{(x|y) : x \in S_1, y \in S_2\}$. Then the distance from S to C is $a + b$. Thus

$$t_{m_1 m_2}(C) \geq t_{m_1}(C_1) + t_{m_2}(C_2).$$

The example in the preceeding paragraph shows that this inequality can be strict. The same inequality holds for the catenation of two linear codes since it is a subcode of their Cartesian product.

3.2 $(u, u+v)$ Construction

Suppose $n_1 = n_2$ and $C_2 \subseteq C_1$. The code C defined by $C = \{(u, u+v) : u \in C_1, v \in C_2\}$ is a $[2n_1, k_1 + k_2, min\{2d_1, d_2\}]$ code (see [6][Ch. 2, Sec. 9]).

Lemma 3.2 *The code C satisfies*

$$t_{m^2}(C) \geq 2t_m(C_1).$$

Proof: Let T be a translate leader of C_1 of maximum weight. Let $S = \{(a,b) : a, b \in T\}$, so S has cardinality m^2. We claim that S is a translate leader of its translate. If not, then there exist $u \in C_1$ and $v \in C_2$ such that $\mathrm{wt}(S + (u, u+v)) < \mathrm{wt}(S)$. Equivalently,

$$\max\{\mathrm{wt}(a+u) + \mathrm{wt}(b+u+v) : a, b \in T\} < max\{\mathrm{wt}(a) + \mathrm{wt}(b)\}.$$

The right hand side of this inequality is just $2\mathrm{wt}(T)$, while the left hand side is the sum of the weights of two other elements of the translate of T. This contradicts the minimality of $\mathrm{wt}(T)$, proving the claim. This also shows that $\mathrm{wt}(S) = 2\mathrm{wt}(T)$, proving the lemma. $\square$

3.3 Repetition

For any integer $r \in \mathbf{N}^*$, the *r-fold repetition* of C_1 is the code $C = \{(c|c|\cdots|c) : c \in C_1\}$, where the code word c is repeated r times. This is a $[rn_1, k_1, rd_1]$ code with $t_m(C) = rt_{rm}(C_1)$.

3.4 Lengthening a Code

A linear code, C, can be lengthened by adjoining a column h to its $k \times n$ generator matrix G, giving rise to the generator matrix $G; h$. The new code is an $[n+1, k]$ code C'. It's codewords consist of vectors of the form $(c, c \cdot b)$, where c is a codeword of C and b is a fixed vector, a new parity check. For any m, the m-covering radius of C' is either $t_m(C)$ or $t_m(C)+1$. We wish to determine when the m-covering radius increases.

Lemma 3.3 *Suppose the code C is lengthened to C' by the addition of a parity check b. Then $t_m(C') = 1 + t_m(C)$ if and only if there is a translate leader $S = \{v_1, \cdots, v_m\}$ of C of weight $t_m(C)$ and a vector $(e_1, \cdots, e_m) \in \mathbf{F}^m$ such that whenever $c \in C$ and $S + c$ is a translate leader, we have $e_i \neq c \cdot b$ for some i such that $\mathrm{wt}(v_i + c)$ is maximal.*

Proof: Suppose $S = \{v_1, \cdots, v_m\}$ is an m-tuple of vectors in $\mathbf{F}^n$. S gives rise to 2^m m-tuples in $\mathbf{F}^{n+1}$, each of the form $S_e = \{(v_1, e_1), \cdots, (v_m, e_m)\}$ for some vector $e = (e_1, \cdots, e_m) \in \mathbf{F}^m$. The weight of S_e can be at most one greater than the weight of S. Thus the m-covering radius increases when the parity check is added if and only if the weight of every translate leader of some maximal weight translate increases. For given S and e, the translate of S_e consists of m-tuples of the form

$$\{(v_1 + c, e_1 + c \cdot b), \cdots, (v_m + c, e_m + c \cdot b)\}$$

where $c \in C$. The weight of this m-tuple is greater than that of $S + c$ exactly when $e_i \neq c \cdot b$ for some i such that $\mathrm{wt}(v_i + c)$ is maximal. □

Corollary 3.4 *Appending a zero parity or an overall parity check to a code increases the m-covering radius by 1.*

Proof: In the first case, take $e_1 = \cdots = e_m = 1$.

In the second case, for any set S, let S' be the odd parity vectors in S and let S'' be the even parity vectors. The maximum weight vectors in S must either all be in S' or all in S''. Suppose S is a maximum weight translate leader and we are in the latter case. We let $e_i = 0$ if $v_i \in S'$, and $e_i = 1$ if $v_i \in S''$. Let $T = S + c$ have the same weight as S. The maximum weight elements of T are in T''. If c has even weight, then $T'' = S'' + c$. For such a vector, $e_i = 1 \neq c \cdot b$. Similarly, if c has odd weight, then $T'' = S' + c$. For such a vector, $e_i = 0 \neq c \cdot b$. If the maximum weight vectors of S are in S', we simply reverse the definition of the e_i. □

4 Lower Bounds

As we have seen, the m-covering radius of a fixed code C, $t_m[n,k]$, $t_m(n,K)$, $k_m[n,t]$, and $K_m(n,t)$ are nondecreasing functions of m. Thus a lower bound for, say, $K_m(n,t)$ implies a bound for $K_{m+1}(n,t)$. Our first bound shows that for $m \geq 2$, the situation for m-covering radii is quite different from that for ordinary covering radii.

Proposition 4.1 *If $m \geq 2$, then the m-covering radius of any code of length n is at least $\lceil n/2 \rceil$.*

Proof: We may assume $m = 2$. Let t be the m-covering radius of C. Let x be any vector of length n, and let $S = \{x, x'\}$. Then for any c,

$$d(x,c) + d(c,x') \geq d(x,x') = n.$$

It follows that one of $d(x,c)$ and $d(x',c)$ is at least $n/2$ □

Thus $K_m(n,t)$ is undefined if $t < n/2$. When this is the case we say $K_m(n,t) = \infty$. There are other circumstances when $K_m(n,t)$ is undefined. For example,

$$K_{2^n}(n, n-1) = \infty.$$

Also $K_m(n,t) = \infty$ if $m > V(n,t)$, since in this case no ball of radius t covers any set of m distinct vectors. More generally, we have the fundamental issue of whether $K_m(n,t)$ is finite for given n, m, t. This is the case if and only if $t_m(\mathbf{F}^n) \leq t$, since the m-covering radius of $\mathbf{F}^n$ lower bounds the m-covering radii of all other codes of dimension n. Thus we want to determine $t_m(\mathbf{F}^n)$. We show that it in fact differs by a constant depending on m but not n from $n/2$.

Theorem 4.2 *For every m there is a constant r_m such that, for every n,*

$$t_m(\mathbf{F}^n) \leq \left\lceil \frac{n + r_m}{2} \right\rceil .$$

Proof: We prove this by induction on n, using the idea behind equation (1). For a given m-tuple, $U = \{u_1, \cdots, u_m\}$, of vectors in $\mathbf{F}^n$, we need to decompose $\mathbf{F}^n$ and U with it so that the resulting pair of m-tuples are covered by balls of small radius. The base case needs to be chosen large enough so that such a decomposition is always possible in the induction step.

Our critical observation is that for any set of three vectors in $\mathbf{F}^2$, there is a vector whose maximum distance to these vectors is one. Let $L \in \mathbf{N}$ be such that whenever

$V = \{v_1, \cdots, v_m\} \subseteq \mathbf{F}^L$, with each $v_i = (v_{1,i}, \cdots, v_{m,i})$, there is a pair of indices i, j so that

$$|\{(v_{k,i}, v_{k,j}) : 1 \leq k \leq m\}| \leq 3.$$

Such an L always exists. At worst, if we take $L = 2^m + 1$, then some "column" $(v_{1,i}, \cdots, v_{m,i})$ must appear twice. In general, however, we are able to do better. For example, for $m = 4$ we can take $L = 4$. As will be seen, the choice of L may affect the constant in the statement of the theorem.

Now suppose $n \geq L$. Then the above fact about L applies to n as well. By permuting the coordinates of $\mathbf{F}^n$, we see that there are a set $U' = \{u'_1, \cdots, u'_m\} \subseteq \mathbf{F}^2$ and a set $U'' = \{u''_1, \cdots, u''_m\} \subseteq \mathbf{F}^{n-2}$, with U_1 containing at most 3 distinct vectors, and $u_i = u'_i | u''_i$ for $i = 1, \cdots, m$. Thus there is a vector $c' \in \mathbf{F}^2$ such that $d(c', u'_i) \leq 2$ for every i, and by induction there is a vector $c'' \in \mathbf{F}^{n-2}$ such that

$$d(c'', u''_i) \leq \left\lceil \frac{n - 2 + r_m}{2} \right\rceil$$

for every i. Letting $c = c'|c''$, it follows that

$$d(c, u_i) \leq \left\lceil \frac{n + r_m}{2} \right\rceil$$

for every i.

For the base case, we have only to take $r_m = L$. □

It is apparent from the proof of the preceeding theorem that the better we can estimate the smallest possible value of L, the better we can bound r_m. The crude estimate in the proof gives $r_m \leq 2^m + 1$. For example, in any set of vectors containing a column with at most one 1 or at most one 0 must have a pair of indices with the property in the proof. Thus we can improve the bound to $r_m \leq 2^m - 2m - 1$. The following theorem gives a lower bound.

Theorem 4.3 *For every m and n satisfying $m \leq 2^n$,*

$$t_m(\mathbf{F}^n) \geq \left\lceil \frac{n + \lfloor \log_n(m) \rfloor - 1}{2} \right\rceil.$$

Proof: Let $k = \lfloor \log(m) \rfloor$, so that $2^k \leq m < 2^{k+1}$. For any $v \in \mathbf{F}^k$, let

$$w_v = \begin{cases} v|0^{n-k} & \text{if } \mathrm{wt}(v) \text{ is even,} \\ v|1^{n-k} & \text{if } \mathrm{wt}(v) \text{ is odd.} \end{cases}$$

There is a set V of m vectors in $\mathbf{F}^n$ that contains every w_v.

Let $c = c_1|c_2 \in \mathbf{F}^n$, with $c_1 \in \mathbf{F}^k$ and $c_2 \in \mathbf{F}^{n-k}$. If the Hamming weight of c_2 is i, then

$$d(w_v, c) = d(v, c_1) + \begin{cases} i & \text{if } \mathrm{wt}(v) \text{ is even,} \\ n-k-i & \text{if } \mathrm{wt}(v) \text{ is odd.} \end{cases}$$

This inequality is an equality in all cases we have been able to compute.

Proposition 4.4 *For $2 \leq m \leq 5$, if n satisfies $m \leq 2^n$, then*

$$t_m(\mathbf{F}^n) = \left\lceil \frac{n + \lfloor \log_n(m) \rfloor - 1}{2} \right\rceil.$$

Proof: In case $m = 2$ or 3, one checks that $t_m(\mathbf{F}^2) = 1$. Given any set of two or three vectors, any pair of columns forms at most three binary pairs. The result follows by the induction argument in Theorem 4.2.

If $m = 4$, it can be seen that in any set of four columns, there is a pair that forms at most three binary pairs. The same induction gives the result, treating the cases $n = 2$ and $n = 3$ as base cases ($t_2(\mathbf{F}^n) = 2$ in both these cases).

The case $m = 5$ is similar, but with $t_5(\mathbf{F}^2) = 2$, $t_5(\mathbf{F}^3) = 2$, and $t_5(\mathbf{F}^4) = 3$ as base cases. □

We conjecture that this relation holds in general.

Conjecture 4.5 *For every $m \geq 2$ and n satisfying $m \leq 2^n$,*

$$t_m(\mathbf{F}^n) = \left\lceil \frac{n + \lfloor \log_n(m) \rfloor - 1}{2} \right\rceil.$$

4.1 The Sphere Bound

We generalize the classical sphere bound, first noted by van Tilborg [8]

Theorem 4.6 *For any (n, K) code C,*

$$K \geq \frac{\binom{2^n}{m}}{\binom{V(n, t_m(C))}{m}}.$$

Thus for any n, t, m,

$$K_m(n,t) \geq \frac{\binom{2^n}{m}}{\binom{V(n,t)}{m}}.$$

Proof: We prove this bound by counting unordered sets of distinct m-tuples of vectors. Each such m-tuple must occur in a neighborhood of radius $t_m(C)$ around at least one code word. The number of m-tuples is 2^n choose m, while the number of m-tuples in a neighborhood of radius $t_m(C)$ is $V(n, t_m(C))$ choose m. □

Corollary 4.7 *If*

$$\binom{2^n}{m} > 2^n \binom{V(n,t)}{m}$$

then $K_m(n,t) = \infty$.

One can also count ordered m-tuples (distinct or not), or not necessarily distinct unordered m-tuples. If we count distinct ordered m-tuples, we get the same bound. In the other two cases we get weaker bounds.

4.2 The Method of Counting Excesses

The sphere bound was improved by van Wee by taking into account some of the overlap between spheres of radius t [9]. We first need a numerical lemma.

Lemma 4.8 *Let* $n \geq t > 0$ *and* $i, j, k, \ell \in \mathbf{N}$, *and* $r = i + j + k + \ell$. *Then*

$$(n+1)^{i+j} t^{k+\ell} + (n+1)^{i+k} t^{j+\ell} - (n+1)^i t^{j+k} (t-1)^\ell \geq 2t^r - (t-1)^r.$$

Proof: First observe that

$$\begin{aligned}
&(n+1)^{i+j} t^{k+\ell} + (n+1)^{i+k} t^{j+\ell} - (n+1)^i t^{j+k} (t-1)^\ell \\
&\quad = \ (n+1)^i ((n+1)^j t^{k+\ell} + (n+1)^k t^{j+\ell} - t^{j+k}(t-1)^\ell) \\
&\quad \geq \ (t+1)^i ((t+1)^j t^{k+\ell} + (t+1)^k t^{j+\ell} - t^{j+k}(t-1)^\ell).
\end{aligned}$$

Thus we can assume $n = t$.

The proof is by a triple induction. The outer induction is on i. Its base case, when $i = 0$, is proved by induction on j. The base case of this induction, when $j = 0$, is proved by induction on k.

Induction on k: We claim that

$$t^{k+\ell} + (t+1)^k t^\ell - t^k (t-1)^\ell \geq 2t^{k+\ell} - (t-1)^{k+\ell}.$$

The base case, when $k=0$, is trivial. For the induction case we have

$$\begin{aligned}
&t^{k+\ell} + (t+1)^k t^\ell - t^k (t-1)^\ell \\
&\quad = \quad t(t^{k-1+\ell} + (t+1)^{k-1} t^\ell - t^{k-1}(t-1)\ell) + (t+1)^k t^\ell - (t+1)^{k-1} t^{\ell+1} \\
&\quad \geq \quad t(2t^{k+\ell-1} - (t-1)^{k+\ell-1} + (t+1)^{k-1} t^\ell \qquad \text{by induction} \\
&\quad = \quad 2t^{k+\ell} - (t-1)^{k+\ell} + (t+1)^{k-1} t^\ell - (t-1)^{k+\ell-1} \\
&\quad \geq \quad 2t^{k+\ell} - (t-1)^{k+\ell}.
\end{aligned}$$

Induction on j: We claim that

$$(t+1)^j t^{k+\ell} + (t+1)^k t^{j+\ell} - t^{j+k}(t-1)^\ell \geq 2t^{j+k+\ell} - (t-1)^{j+k+\ell}.$$

The base case has been proved. For the induction case we have

$$\begin{aligned}
&(t+1)^j t^{k+\ell} + (t+1)^k t^{j+\ell} - t^{j+k}(t-1)^\ell \\
&\quad = \quad t((t+1)^{j-1} t^{k+\ell} + (t+1)^k t^{j-1+\ell} - t^{j-1+k}(t-1)^\ell) + (t+1)^j t^{k+\ell} - (t+1)^{j-1} t^{k+\ell+1} \\
&\quad \geq \quad t(2t^{j+k+\ell-1} - (t-1)^{j+k+\ell-1}) + (t+1)^{j-1} t^{k+\ell} \\
&\quad = \quad 2t^{j+k+\ell} - (t-1)^{j+k+\ell} + (t+1)^{j-1} t^{k+\ell} - (t-1)^{j+k+\ell-1}) \\
&\quad \geq \quad 2t^{j+k+\ell} - (t-1)^{j+k+\ell}.
\end{aligned}$$

Induction on i: We claim that

$$(t+1)^i((t+1)^j t^{k+\ell} + (t+1)^k t^{j+\ell} - t^{j+k}(t-1)^\ell) > 2t^{i+j+k+\ell} - (t-1)^{i+j+k+\ell}.$$

By induction, it suffices to show this in case $i=1$. By the previous section of the proof we have

$$\begin{aligned}
&(t+1)((t+1)^j t^{k+\ell} + (t+1)^k t^{j+\ell} - t^{j+k}(t-1)^\ell) \\
&\quad \geq \quad (t+1)(2t^{j+k+\ell} - (t-1)^{j+k+\ell}) \\
&\quad = \quad 2t^{j+k+\ell+1} - (t-1)^{j+k+\ell+1} + 2t^{j+k+\ell} + (t-1)^{j+k+\ell+1} - (t+1)(t-1)^{j+k+\ell} \\
&\quad = \quad 2t^{j+k+\ell+1} - (t-1)^{j+k+\ell+1} + 2t^{j+k+\ell} - 2(t-1)^{j+k+\ell} \\
&\quad \geq \quad 2t^{j+k+\ell+1} - (t-1)^{j+k+\ell+1}.
\end{aligned}$$

This proves the lemma. ∎

Theorem 4.9 *For any n, m, t with $n > t$,*

$$K_m(n,t) \geq \frac{\sigma 2^{nm} + \epsilon\binom{2^n}{m}}{\sigma V(n,t)^m + \epsilon\binom{V(n,t-1)}{m}},$$

where

$$\sigma = (n+1)^m - 2t^m + (t-1)^m$$

and

$$\epsilon = m!\left((t+1)\left\lceil\frac{(n+1)^m}{t+1}\right\rceil - (n+1)^m\right).$$

Proof: The proof combines counting of unordered sets of m-tuples of distinct vectors and ordered m-tuples of not necessarily distinct vectors. We use the following notation.

1. $A = \{(x^1, \cdots, x^m) : \min_{c\in C} \max_i d(x^i, c) = t\}$, the set of ordered m-tuples of not necessarily distinct vectors with maximum distance from C.

2. $A' = \{\{x^1, \cdots, x^m\} : \min_{c\in C} \max_i d(x^i, c) = t,$ and $x^i \neq x^j$ if $i \neq j\}$, the set of unordered sets of m-tuples of distinct vectors with maximum distance from C.

3. $X_i = \{(x^1, \cdots, x^m) :$ there are exactly $i+1$ code words $c \in C$ with $\max_i(x^i, c) \leq t\}$, the set of ordered m-tuples covered by $i+1$ code words.

4. For any set $V \in \mathbf{F}^n$, $E(V) = \sum_i |X_i \cap V|$, the excess of V. This is the number of extra times the elements of V are counted if we add the sizes of the neighborhoods of radius t all code words.

5. For any $x = (x^1, \cdots, x^m) \in \mathbf{F}^{nm}$ and integer r,

$$B_r(x) = \{(y^1, \cdots, y^m) : \text{ for every } i,\ d(x^i, y^i) \leq r\}.$$

We claim the following hold:

a.
$$\binom{2^n}{m} - |C|\binom{V(n,t-1)}{m} \leq |A'|. \tag{2}$$

b. If $y \in A$, then
$$\epsilon/m! \leq E(B_1(y)). \tag{3}$$

c. For any set V,

$$\sum_{y\in A} |V \cap B_1(y)| = \sum_{x\in V} |A \cap B_1(x)|. \tag{4}$$

d. If $x \in X_i$, $i \geq 1$, then

$$|A \cap B_1(x)| \leq \sigma. \tag{5}$$

Suppose these four equations hold. Then

$$\begin{aligned}
\epsilon\left(\binom{2^n}{m} - |C|\binom{V(n,t-1)}{m}\right) &\leq \epsilon|A'| \text{ by equation (2)} \\
&\leq (\epsilon/m!)|A| \\
&\leq \sum_{y\in A}\sum_{i\geq 0} i|X_i \cap B_1(y)| \text{ by equation (3)} \\
&= \sum_{i\geq 0} i \sum_{x\in X_i} |A \cap B_1(x)| \text{ by equation (4)} \\
&\leq \sum_{i\geq 0} i\sigma|X_i| \text{ by equation (5)} \\
&= \sigma(|C|V(n,t)^m - 2^{nm}).
\end{aligned}$$

Solving for $|C|$ then completes the proof of the theorem.

Proof of equation (2): This follows since $\binom{2^n}{m} - |A'|$ is the number of unordered m-tuples of distinct vectors within distance $t-1$ of C.

Proof of equation (3): Observe that

$$\begin{aligned}
E(B_1(y)) + |B_1(y)| &= \{(x,z) \in C \times B_1(y) : \text{ for } i = 1, \cdots, m,\ d(z^i, c) \leq t\} \\
&= \sum_{c\in C}\prod_{i=1}^{m} |B_1(y_i) \cap B_t(c)|.
\end{aligned}$$

Furthermore,

$$B_1(y_i) \cap B_t(c) = \begin{cases} n+1 & \text{if } d(c, y_i) \leq t-1 \\ t+1 & \text{if } d(c, y_i) = t \text{ or } t+1 \\ 0 & \text{if } d(c, y_i) \geq t+2. \end{cases}$$

Since $y \in A$, for every $c \in C$ there is at least one i for which this is 0 or $t+1$. Thus the product is always divisible by $t+1$. For every y, $|B_1(y)| = (n+1)^m$. Therefore

$|E(B_1(y))| \equiv -(n+1)^m \bmod (t+1)$. Since $|E(B_1(y))|$ is nonnegative, it must be at least $\epsilon/m!$.

Proof of equation (4): We have

$$\begin{aligned} \sum_{y \in A} |V \cap B_1(y)| &= |\{(x,y) : x \in V, y \in A, d(x,y) \le 1\}| \\ &= \sum_{x \in V} |A \cap B_1(x)|. \end{aligned}$$

Proof of equation (5): If $x \in Z_i$, $i > 0$, then there are at least two distinct $c, d \in C$ such that for all i, $d(x^i, c) \le t$ and $d(x^i, d) \le t$. We have

$$|A \cap B_1(x)| \le (n+1)^m - \lambda,$$

where

$$\begin{aligned} \lambda &= |B_1(x) \cap (B_{t-1}(c^n) \cup B_{t-1}(d^n))| \\ &= |B_1(x) \cap B_{t-1}(c^n)| + |B_1(x) \cap B_{t-1}(c^n)| - |B_1(x) \cap B_{t-1}(c^n) \cap B_{t-1}(d^n)| \quad (6) \end{aligned}$$

by the inclusion/exclusion principle. Furthermore, we have

$$|B_1(x) \cap B_{t-1}(c^n)| = \prod_i |B_1(x^i) \cap B_{t-1}(c)|$$

and similarly for the other two terms on the right-hand side of equation (6). It can be seen that the only four possibilities for the vector

$$(|B_1(x^i) \cap B_{t-1}(c)|, |B_1(x^i) \cap B_{t-1}(d)|, |B_1(x^i) \cap B_{t-1}(c) \cap B_{t-1}(d)|)$$

are $(n+1, n+1, n+1), (n+1, t, t), (t, n+1, t), (t, t, s)$ for $s \le t-1$. It follows that for some integers i, j, k, ℓ, with $i + j + k + \ell = n$,

$$\lambda \ge (n+1)^{i+j} t^{k+\ell} + (n+1)^{i+k} t^{j+\ell} - (n+1)^i t^{j+k} (t-1)^\ell.$$

By Lemma 4.8, $\lambda \ge 2t^n - (t-1)^n$. This proves the theorem. $\square$

5 Large Values

In this section we consider bounds in various cases of large values of the parameters. When $t = n$, every codeword covers every vector, so a code of size 1 will m-cover $\mathbf{F}^n$ for every m.

When $t = n-1$, any code of size $m+1$ will m-cover $\mathbf{F}^n$. To prove this we first need a lemma.

Lemma 5.1 *Let x be a natural number, $x > 0$, and let m and k be natural numbers. Define*

$$f_{k,m}(x) = \sum_{i=0}^{k} (-1)^i \binom{k}{i} (x-i)^m.$$

Then $f_{k,m}(x) = 0$ if and only if $k \geq m+1$.

Proof: For $m > 0$, we can write

$$\begin{aligned} f_{k,m}(x) &= x \sum_{i=0}^{k} (-1)^i \binom{k}{i} (x-i)^{m-1} - \sum_{i=0}^{k} i(-1)^i \binom{k}{i} (x-i)^{m-1} \\ &= x f_{k,m-1}(x) + k f_{k-1,m-1}(x+1). \end{aligned} \tag{7}$$

First we assume $k \geq m+1$ and prove the "if" part by induction on m. For $m = 0$ we have

$$\begin{aligned} f_{k,0}(x) &= \sum_{i=0} (-1)^i \binom{k}{i} \\ &= (1-1)^k \\ &= 0 \end{aligned}$$

if $k > 0$. When $m > 0$, it follows by induction from equation (7) that $f_{k,m}(x) = 0$.

Now we assume $k \leq m$. We prove that $f_{k,m}(x) > 0$. For $m = 0$, we must have $k = 0$, and $f_{0,0}(x) = 1$. For $m > 0$, it follows by induction from equation (7) that $f_{k,m}(x) > 0$, since both terms on the right hand side are nonnegative and the second term is positive. □

Theorem 5.2 *For all natural numbers n and m, we have $K_m(n, n-1) = m+1$.*

Proof: Let C be any code. Each neighborhood of radius $n-1$ around a codeword c omits precisely one vector, the complement of c. Thus the intersection of the neighborhoods of radius $n-1$ around any j codewords omits precisely j vectors. If $|C| = k$, it follows from the inclusion/exclusion principle that the number of m-tuples of vectors covered by the neighborhoods of radius $n-1$ around the code words of C is precisely $2^{mn} - f_{k,m}(2^n)$. The theorem follows immediately from Lemma 5.1. □

Corollary 5.3 *For all natural numbers n, $t \le n-2$, and m, we have $K_m(n,t) \ge m+1$.*

6 Multicovering Radii of Particular Codes

As a trivial example, the m-covering radius of the repetition code $C = \{0^n, 1^n\}$ is n, since the smallest ball around a codeword that covers the 2 element set $\{0^n, 1^n\}$ has radius n.

6.1 Hamming Codes

It is well known that the ordinary covering radius of a Hamming code is 1, i.e. minimal [6]. Here we prove that the m-covering radius of a Hamming code is nearly minimal. We denote the rth Hamming code by H_r. This is a $[2^r-1, 2^r-r-1, 3]$ code, with the $r \times (2^r-1)$ matrix whose columns are all nonzero vectors of length r as parity check matrix. It follows that for some ordering of the coordinates of H_r,

$$H_r = \{(v+u, u, a) : v \in H_{r-1} \text{ and } a = \mathrm{wt}(u) \bmod 2\}.$$

When $r = 2$, H_r is just the repetition code of length 3, so $t_m(H_2) = 3$ if $m \ge 2$.

Proposition 6.1 *For any $m \ge 2$, there is a constant c_m such that for any $r \ge 2$*

$$2^{r-1} \le t_m(H_r) \le 2^{r-1} + c_m r.$$

Proof: The lower bound is from Proposition 4.1. The upper bound is proved by induction. Let r_m be the constant of Theorem 4.2. We take $c_m = \max(1, \lceil r_m/2 \rceil)$. It is easily checked that the inequality holds when $r = 2$. If $r > 2$ and

$$\{(x_i, y_i, b_i) \in \mathbf{F}^{2^{r-1}-1} \times \mathbf{F}^{2^{r-1}-1} \times \mathbf{F} : i = 1, \cdots, m\},$$

then there is $(u, a) \in \mathbf{F}^{2^r-1} \times \mathbf{F}$ such that

$$d((u,a),(y_i,b_i)) \le \left\lceil \frac{2^{r-1}+r_m}{2} \right\rceil.$$

The inequality follows by taking, by induction, $v \in H_{r-1}$ so that

$$d(v, x_i + u) \le t_m(H_{r-1}).$$

$\square$

For $m = 4$ or 5, we can take $r_m = 1$. For $m = 3$, we have $\lceil r_m/2 \rceil = 0$. In this case we can improve the induction to show that

$$2^{r-1} \le t_m(H_r) \le 2^{r-1} + 1.$$

For $m = 2$ we have a precise answer. We first treat H_3, proving an apparently stronger result than necessary that will be useful in the proof of the general case.

Lemma 6.2 *Any pair of vectors in $\mathbf{F}^7$ is covered by at least two distinct codewords within radius 4.*

Proof: Suppose we are given $w_i = (x_i, y_i, b_i) \in \mathbf{F}^7$, with $x_i, y_i \in \mathbf{F}^4$ and $b_i \in \mathbf{F}$, $i = 1, 2$. There are several cases to consider.

Suppose either $\mathrm{wt}(y_i, b_i)$ is even for at least one $i = 1$ or 2, or both $\mathrm{wt}(y_1, b_1)$ and $\mathrm{wt}(y_2, b_2)$ are odd and $d((y_1, b_1), (y_2, b_2)) \le 2$. Consider choices of $u \in \mathbf{F}^4$ and $a \in \mathbf{F}$ such that

$$d((u, a), (y_i, b_i)) \le 2, \text{ for } i = 1, 2 \text{ and } \mathrm{wt}(u, a) \text{ even}.$$

There is a set of three such choices with no two us complements of each other. For any such (u, a), $\max_{v \in H_2} d(v, x_i + u) = 3$ only if $\{x_i + u\} = \{(0, 0, 0), (1, 1, 1)\}$. This can happen only for either a single u or a single complementary pair of us. Hence there are at least two such choices of (u, a) for which there is a $v \in H_2$ satisfying $d(v, x_i + u) \le 2$. Each $(v + u, u, a)$ is an element of H_3 whose distance from each w_i is at most 4.

On the contrary, suppose $\mathrm{wt}(y_i, b_i)$ is odd for $i = 1, 2$ and $d((y_1, b_1), (y_2, b_2)) = 4$. That is, (y_1, b_1) and (y_2, b_2) are complementary. There are four even weight pairs (u, a) such that $d((u, a), (y_1, b_1)) = 1$ and $d((u, a), (y_2, b_2)) = 3$. For each such (u, a), there is a $v \in H_2$ such that $(d(v, x_1 + u), d(v, x_2 + u)) \in \{(1, 0), (1, 1), (2, 0), (2, 1), (3, 0)\}$. In any case, $d((v + u, u, a), w_i) \le 4$, and the four choices of (u, a) give us the lemma. $\square$

Proposition 6.3 *For any $r \ge 3$*

$$t_2(H_r) = 2^{r-1}.$$

Proof: The proof is by induction on r. We prove the stronger statement that any pair of vectors in $\mathbf{F}^{2^r-1}$ is covered by at least two distinct codewords of H_r within radius 2^{r-1}. The base case, $r = 3$, is given by Lemma 6.2.

Let $r > 3$ and suppose we are given a pair of vectors

$$w_i = (x_i, y_i, b_i), \text{ where} x_i, y_i \in \mathbf{F}^{2^{r-1}-1} \text{ and } b_i \in \mathbf{F} \text{ for } i = 1, 2.$$

We need to show that there are two vectors

$$(v + u, u, a) \in H_r$$

whose distances from each w_i are at most $2^{r-1} + 1$. We consider several cases separately.

Suppose first that $\mathrm{wt}(y_i, b_i)$ is even for $i = 1$ or 2. Then there is an even weight

$$(u, a) \in \mathbf{F}^{2^{r-1}}$$

whose distance from each (y_i, b_i) is at most 2^{r-2}. There are two vs whose distances from each $x_i + u$ are at most $t_2(H_{r-1})$. Thus for each i,

$$\begin{aligned} d((v + u, u, a), (x_i, y_i, b_i)) &\leq t_2(H_{r-1}) + 2^{r-2} \\ &= 2^{r-1}. \end{aligned}$$

Next suppose that both $\mathrm{wt}(y_1, b_1)$ and $\mathrm{wt}(y_2, b_2)$ are odd and that

$$d((y_1, b_1)(y_2, b_2)) \leq 2^{r-1} - 2.$$

Then there is a

$$(u, a) \in \mathbf{F}^{2^{r-1}}$$

of even weight such that

$$d((u, a), (y_1, b_1) \leq 2^{r-2} - 1$$

and

$$d((u, a), (y_2, b_2) \leq 2^{r-2} - 1.$$

There are two choices of

$$v \in \mathbf{F}^{2^{r-1}}$$

so that

$$d(v, x_i + u) \leq t_2(H_{r-1}).$$

The bound follows.

On the other hand, suppose that both $\mathrm{wt}(y_1, b_1)$ and $\mathrm{wt}(y_2, b_2)$ are odd and

$$d((y_1, b_1), (y_2, b_2)) = 2^{r-1}.$$

That is, (y_2, b_2) is the complement of (y_1, b_1). Let

$$u \in \mathbf{F}^{2^{r-1}-1}$$

satisfy

$$d((y_i, b_i), (u, 0)) = 2^{r-2}$$

(thus z has odd weight). Note that there are at least 21 choices of such u. Let $v \in H_{r-1}$ satisfy

$$\begin{aligned} d(v, x_i + u) &\leq t_2(H_{r-1}) \\ &= 2^{r-2} \end{aligned} \tag{8}$$

for $i = 1, 2$. If this inequality is strict for $i = 1, 2$, then

$$d((v + u, u, 1), w_i) \leq 2^{r-1}.$$

Suppose on the contrary (and without loss of generality) that $d(v, x_1 + u) = 2^{r-2}$. Let

$$S = \mathrm{supp}(v + x_1 + u) \cap \mathrm{supp}(v + x_2 + u).$$

If $S \neq \emptyset$, let

$$e \in \mathbf{F}^{2^{r-1}-1}$$

be a vector of weight one whose support is in S. Then

$$d(v + u + e, x_i) \leq 2^{r-2} - 1$$

and

$$d((u + e, 0), (y_i, b_i)) \leq 2^{r-2} + 1,$$

so

$$d((v + u + e, u + e, 0), w_i) \leq 2^{r-1}.$$

If $S = \emptyset$, we let

$$T = \mathrm{supp}(v + x_1 + u) \cap \mathrm{supp}(y_2 + u).$$

If $T \neq \emptyset$, let

$$e \in \mathbf{F}^{2^{r-1}-1}$$

be a vector of weight one whose support is in T. Then

$$\begin{aligned} d((v+u+e, u+e, 0), w_1) &= \mathrm{wt}(v+u+e+x_1) + \mathrm{wt}((u+e,0)+(y_1,b_1)) \\ &\leq 2^{r-2} - 1 + 2^{r-2} + 1 \\ &= 2^{r-1}. \end{aligned}$$

So let us suppose that $S = T = \emptyset$. We have

$$\mathrm{wt}(v+x_1+u) = 2^{r-2},$$

and

$$\mathrm{wt}(y_2+u) \in \{2^{r-2}-1, 2^{r-2}\}.$$

The condition on the supports then implies that $\mathrm{wt}(y_2+u) = 2^{r-1}-1$ and y_2+u is the complement of $v+x_1+u$. Thus y_2 is the complement of $v+x_1$. Hence $v+x_1 = y_1$. However, by induction there are at least two choices of v that satisfy equation (8). (This is where we need the stronger induction hypothesis.) For at least one of these, $S \neq \emptyset$ or $T \neq \emptyset$, allowing us to achieve the desired bound. □

7 Conclusions and Open Problems

We have introduced a natural generalization of the covering radius of a code. We have described many of the basic properties of multicovering radii. In many cases this was a matter of generalizing earlier results on covering radii to this new setting. The subject of covering radii is large and one can attempt to duplicate all the work that has been done on this subject in this new setting. In particular, we would like better bounds on various fundamental quantities: the size of the smallest code with specified length and m-covering radius; the minimum m-covering radius for a code a certain size and length.

We would like to see precise values for these quantities for small length codes. This is, to a large extent, a matter of working out the m-covering radii for many of the standard codes. We have begun this sort of analysis by considering Hamming codes, but our analysis even in this case is not complete. It is apparent from what has been done here that the situation for multicovering radii is far more complicated than for ordinary covering radii.

Finally, this work was motivated by work in the cryptanalysis of stream ciphers. It became apparent that to prove an existence theorem for stream ciphers secure against a very general type of attack we need a class of efficiently generated codes that have small multicovering radii. Hamming codes satisfy the second requirement but, unfortunately, not the first. Reed-Muller codes of bounded degree satisfy the first requirement, but, as yet, we do not know whether they satisfy the second. Moreover, known bounds on their ordinary covering radii were sufficient to acquire some useful cryptologic results. Thus we consider the determination of sharp bounds on the multicovering radii of Reed-Muller codes to be a major open problem.

References

[1] G.D. Cohen, M.G. Karpovsky, H.F. Mattson, Jr., and J.R. Schatz, "Covering radius – survey and recent results," *IEEE Trans. Info. Theory* vol. IT-31, pp. 328-343, 1985.

[2] G.D. Cohen, S.N. Litsyn, A.C. Lobstein, and H.F. Mattson, Jr., "Covering Radius 1985-1994," Technical Report 94 D 025, Dept. Informatique, Ecole Nationale Supérieure des Télécommunications, 1994.

[3] A. Klapper, "The Vulnerability of Geometric Sequences Based on Fields of Odd Characteristic," *Journal of Cryptology* vol. 7 pp. 33-51, 1994.

[4] A. Klapper, "On the Existence of Secure Feedback Registers," in *Advances in Cryptology: Proc. Eurocrypt '96, Lecture Notes in Computer Science Vol. 388*, Springer-Verlag: Berlin, pp. , 1996.

[5] A. Klapper and M. Goresky, "Feedback Shift Registers, Combiners with Memory, and 2-Adic Span," to appear, *Journal of Cryptology.*

[6] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error Correcting Codes,* North-Holland: Amsterdam, 1977.

[7] J.L. Massey, "Shift register sequences and BCH decoding," *IEEE Trans. Info. Theory* vol. IT-15, pp. 122-127, 1969.

[8] H.C.A. van Tilborg, *Uniformly Packed Codes.* Eindhoven, The Netherlands: Eindhoven Tech. Univ., 1976.

[9] G.J.M. van Wee, "Improved sphere bounds on the covering radius of codes," *IEEE Trans. Info. Theory* vol. 34, pp. 237-245, 1988.