Improved Lower Bounds for Multicovering Codes

Andrew Klapper*

March 4, 1999

Abstract

The *m-covering radius* of a code is a recent generalization of the covering radius of a code. It is the smallest t such that every m-tuple of vectors is contained in a ball of Hamming radius centered at some codeword. We derive new lower bounds for the size of the smallest code that has a given length and m-covering radius.

1 Introduction

The purpose of this paper is to give improved lower bounds on the size of the smallest codes exhibiting a given multicovering radius. These bounds are improvements on generalized sphere bounds for multicovering radii [3].

Multicovering radii, which were introduced recently [3], are defined as follows. We let $\mathbf{F} = \{0, 1\}$ denote the field with two elements. We also denote the Hamming distance between two vectors u and v by $\mathrm{dist}(u, v)$ and the complement of a vector v by $\bar{v}$.

Definition 1.1 *Let C be a binary code of length n. Let m be an positive integer. The* m-covering radius *of C, denoted by $t_m(C)$, is the smallest integer t such every m-tuple of vectors in $\mathbf{F}^n$ is contained in a ball of radius t around at least one codeword in C. That is,* $\forall v_1, \cdots, v_m \in \mathbf{F}^n : \exists c \in C : \forall i = 1, \cdots, m : \mathrm{dist}(c, v_i) \le t$.

*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.

This is a natural generalization of the classical notion of covering radius, which is exactly the case when $m = 1$ [1, 2]. In this paper, we are interested in the size of the smallest code with a given length n and m-covering radius at most t, denoted $K_m(n,t)$. For linear codes, the dimension of the smallest code with length n and m-covering radius at most t is denoted $k_m(n,t)$. There may be no code with a given length n and with m-covering radius less than or equal to a given t. In this case we say $K_m(n,t) = k_m(n,t) = \infty$.

We recall several known facts concerning $K_m(n,t)$.

Proposition 1.2 *(See [3]) For any $n, m, t \in \mathbf{N}^*$, we have*

1. $K_m(n,t) \leq K_{m+1}(n,t)$ *and* $k_m[n,t] \leq k_{m+1}[n,t]$;
2. $K_m(n,t) \geq K_m(n,t+1)$ *and* $k_m[n,t] \geq k_m[n,t+1]$;
3. *If* $2 \leq m \leq 2^n$ *and*
$$t < \left\lceil \frac{n + \lfloor \log_2(m) \rfloor - 1}{2} \right\rceil,$$
then $K_m(n,t) = k_m(n,t) = \infty$;
4. *(The sphere bound)*
$$K_m(n,t) \geq \frac{\binom{2^n}{m}}{\binom{V(n,t)}{m}};$$
5. $K_m(n,n-1) = m+1$.
6. *If* $t \leq n-1$, *then* $K_m(n,t) \geq m+1$;
7. *If* $n = 2^r - 1$, *then there is a constant* c_m *such that* $k_m(n, 2^{r-1} + c_m) \leq 2^r - r - 1$ *(Hamming codes). Also,* $c_2 = 0$ *and* $c_3 = c_4 = c_5 = 1$.

2 Improved Bounds

The sphere bound (Proposition 1.2.4) is proved by counting the number of m-tuples of vectors that can be covered by a single codeword, and dividing into the total number of m-tuples of vectors. For $m \geq 2$, we can improve the bound by only considering special m-tuples. We want a large class of m-tuples such that very few m-tuples can be covered by any particular codeword. The classes we consider are the sets of translates of fixed m-tuples. If Γ is a set of vectors and c is a vector, we $c + \Gamma = \{c + v : v \in \Gamma\}$.

Definition 2.1 *Let D be a set of vectors in $\mathbf{F}_2^n$ and let $t > 0$. Then*

$$\Gamma_t(D) = \{c \in \mathbf{F}_2^n : \forall u \in D : \mathrm{dist}(u, c) \leq t\}.$$

Let $m = |D|$. Every code with m-covering radius t or less must cover every translate of D. There are 2^n such translates. A single codeword c, however, covers a translate $u + D$ only if $c + u$ covers D. Thus each c covers at most $|\Gamma_t(D)|$ translates of D. Hence the cardinality of C must be at least $2^n/|\Gamma_t(D)|$. This proves the following bound.

Theorem 2.2 *For any $m \geq 1$, $n \geq 1$, $t \geq 0$, and set $D \subseteq \mathbf{F}_2^n$ with $|D| = m$,*

$$K_m(n, t) \geq \frac{2^n}{|\Gamma_t(D)|}.$$

Thus we can prove lower bounds on $K_m(n, t)$ by choosing D so that $\Gamma_t(D)$ is small. We next construct such D based on invertible matrices each of whose entries is plus or minus one.

Now suppose H is an invertible $s \times s$ matrix each of whose entries is one or minus one. It can be seen that such a matrix exists for every s. Let $v_1, v_2, \cdots v_s$ be the rows of H and let $v_i = (v_{i,1}, \cdots, v_{i,s})$. Let $k > 0$ and $n = ks$. We construct a set D of $m = 2s$ vectors. Define $\phi : \{\pm 1\} \to \{0, 1\}$ by $\phi(1) = 0$ and $\phi(-1) = 1$. For each $i = 1, \cdots, s$, let

$$u_i = \phi(v_{i,1})^k | \cdots | \phi(v_{i,s})^k.$$

We set $D = \{u_i\} \cup \{\bar{u}_i\}$. We have $m \geq 2$, so we let $t \geq n/2$.

Suppose $c = (c_1, \cdots, c_n) \in \Gamma_t(D)$. For each $j = 1, \cdots, s$, let a_j be the number of 1's in the block $c_{k(j-1)+1}, \cdots, c_{kj}$. The distance from c to each u_i is completely determined by the a_j. In fact,

$$\mathrm{dist}(c, u_i) = \sum_{v_{i,j}=1} a_j + \sum_{v_{i,j}=-1} (k - a_j).$$

Equivalently, if d_i is the number of minus ones in v_i,

$$\mathrm{dist}(c, u_i) - kd_i = \sum_{j=1}^{s} v_{i,j} a_j. \tag{1}$$

For a fixed value of $\mathrm{dist}(c, u_i)$, we want to think of this as a linear equation in the a_js.

It is necessary that both $\mathrm{dist}(c, u_i) \leq t$, and $\mathrm{dist}(c, \bar{u}_i) \leq t$. It follows that $\mathrm{dist}(c, u_i) \geq n - t$. Thus

$$n - t - kd_i \leq \sum_{j=1}^{s} v_{i,j} a_j \leq t - kd_i.$$

In particular, there are $2t-n+1$ possible values for $\sum_{j=1}^{s} v_{i,j}a_j$. If we make a choice of such a value for each i, then we have a system of s equations in the s unknowns a_j, and the matrix of this system is H. Thus there is a unique solution over the rational numbers, and so at most one solution with a_i an integer between 0 and k.

Once we have determined a solution $\{a_j\}$ to the system of equations, a particular c is determined by a choice of which a_j of the k bits in the jth block will be ones. There are

$$\binom{k}{a_j} \leq \binom{k}{\lfloor k/2 \rfloor}$$

possible such choices. In summary, we have $(2t-n+1)^s$ choices for $\{\mathrm{dist}(c,u^i)\}$ and at most $\binom{k}{\lfloor k/2\rfloor}^s$ possible cs for each choice.

Theorem 2.3 *Let m and n be integers with m even and $m/2$ dividing n. Then*

$$K_m(n,t) \geq \frac{2^n}{(2t-n+1)^{m/2}\binom{2n/m}{\lfloor n/m\rfloor}^{m/2}}.$$

Proof: Let $s=m/2$ and $k=n/s$. By the above argument, with these parameters there is a set D with m elements such that $|\Gamma_m(D)|$ is at most

$$(2t-n+1)^s\binom{k}{k/2}^s.$$

It then follows from Theorem 2.2 that

$$K_m(n,t) \geq \frac{2^n}{(2t-n+1)^s\binom{k}{k/2}^s}.$$

Writing this in terms of m and n gives the theorem. □

Next we consider what happens if $2t-n$ is held constant. By Proposition 1.2.3, this is includes the case when t is as small as possible.

Corollary 2.4 *Let d be a fixed constant. Let m be an even positive integer. Then there is a constant c depending only on d such that for every n that is a multiple of $m/2$,*

$$K_m\left(n, \left\lceil\frac{n+d}{2}\right\rceil\right) \geq c\left(\frac{n}{\pi m}\right)^{m/4}.$$

Proof: In this case $2t-n+1 \leq d+3$. Also, by Stirling's formula,

$$\binom{k}{k/2} \sim 2^k\sqrt{\frac{2\pi}{k}}.$$

The result follows. □

3 Conclusions

We have given asymptotic lower bounds on the size of the smallest code with given length and m-covering radius for even m. If m is odd, then we obtain bounds for $K_m(n,t)$ since $K_m(n,t) \geq K_{m-1}(n,t)$. However, better bounds may be possible. In fact for even m as well as odd it's clear from our arguments that the bounds given are not tight Some improvement might be accomplished by more precise bounds on the minimum of $|\Gamma_t(D)$ over all D of cardinality m. Even this, however, is unlikely to lead to optimal bounds for $K_m(n,t)$.

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," Dept. Informatique, Ecole Nationale Supérieure des Télécommunications, Technical Report 94 D 025, 1994.

[3] A. Klapper, "The Multicovering radii of codes," *IEEE Trans. Info. Theory* vol. , pp. , 1997.