Improved Multicovering Bounds from Linear Inequalities and Supercodes

Andrew Klapper

***Abstract*— The multicovering radii of a code are natural generalizations of the covering radius in which the goal is to cover all m-tuples of vectors for some m as cheaply as possible. In this paper we describe several techniques for obtaining lower bounds on the sizes of codes achieving a given multicovering radius. Our main method is a generalization of the method of linear inequalities based on refined weight distributions of the code. We also obtain a linear upper bound on the 2-covering radius. We further study bounds on the sizes of codes with a given multicovering radius that are subcodes of a fixed code. We find, for example, constraints on parity checks for codes with small ordinary covering radius.**

Keywords: Covering radius, error correcting code, weight distribution, linear inequality, supercode.

I. Introduction and Definitions

The method of linear inequalities has been used previously to obtain lower bounds on the size of a code with a given covering radius [2], [11]. The purpose of this paper is to extend these techniques to obtain lower bounds on the size of a code with a given multicovering radius.

The general definitions and basic properties of covering radii can be found in Cohen, Honkala, Litsyn, and Lobstein's book [2]. Let $\mathbf{F} = \{0, 1\}$ and let $C \subseteq \mathbf{F}^n$ be a code of length n. For any positive integer m 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 [4]. We denote the m-covering radius of a code C by $R_m(C)$. Thus $R_1(C)$ is the ordinary covering radius. If $\mathbf{x}$ is a vector, then $\overline{\mathbf{x}}$ denotes the bitwise complement of $\mathbf{x}$. If $\mathbf{x}$ and $\mathbf{y}$ are vectors, then $\mathbf{x}|\mathbf{y}$ denotes the concatenation of $\mathbf{x}$ and $\mathbf{y}$. We denote by $\mathrm{d}(\mathbf{x}, \mathbf{y})$ the Hamming distance between $\mathbf{x}$ and $\mathbf{y}$.

In general we are interested in various extremal values associated with this notion: $t_m(n) = R_m(\mathbf{F}^n)$, the smallest m-covering radius among length n codes; $t_m(n, k)$, the smallest m-covering radius among (n, k) codes; $\ell_m(a, t)$, the smallest length of a linear code with codimension a and m-covering radius t; and $K^m(n, t)$, the smallest cardinality of a length n code with m-covering radius t. It is the latter quantity that we study in this paper, deriving new lower bounds using inequalities for linear combinations of the weight distributions of codes. In the case $m = 2$, we also obtain an upper bound on $K^2(n, t)$ that is twice the lower bound.

As with the ordinary covering radius, a variety of bounds are known for these quantities [4], [5], but precise values are only known in cases of small length. By bounding the number of m-sets that can be covered by a given codeword, one obtains a straightforward generalization of the sphere bound [4], namely

$$K^m(n, t) \geq \frac{\binom{2^n}{m}}{\binom{V(n,t)}{m}}. \qquad (1)$$

This bound was improved by considering only pessimal m-sets [5].

Theorem 1: Let m, n, and t be integers with m even and $m/2$ dividing n and $n/2 \leq t \leq n$. Then

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

The method of linear inequalities, due to Zhang [11], is a technique for obtaining lower bounds on the size of a code if a linear inequality for its generalized weight distribution (for each vector $\mathbf{x}$ and each nonnegative integer i, the number of codewords whose distance from $\mathbf{x}$ equals i) is known. In this paper we generalize the method of linear inequalities (§II). We treat $\mathbf{F}^n$ as a product and consider the distribution of codewords $\mathbf{c}$ with the distance from each component of $\mathbf{c}$ to the correspondng component of $\mathbf{x}$ specified. Linear inequalities on these weight distributions again give rise to lower bounds on the size of a code. The technique can even be applied if the linear inequalities hold only for $\mathbf{x}$ in some linear code containing the target code. In §III we combine this approach with an approach to finding lower bounds from extremal sets to obtain new lower bounds for the m-covering radius of a code. In §IV we obtain tight bounds on the size of the smallest code with a given 2-covering radius using a result of Alon, Bergmann, Coppersmith, and Odlyzko [1], and combine this result with the method of linear inequalities to obtain improved bounds on codes with given m-covering radius for arbitrary $m > 2$. As an example, we apply these techniques to obtain bounds on the 1-, 4-, and 6-covering radii of a code with a single parity check. We see, for example, that a minimal size code with length n and ordinary covering radius 1 can only have parity checks whose weights are close to $n/2$. Also, a minimal size code with length n and ordinary covering radius 2 can only have parity checks whose weights are close to $(n \pm \sqrt{n})/2$.

II. Supercodes and Linear Inequalities

In this section we consider a fixed linear code C' and derive a lower bound on the size of a code contained in C' that has

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-9400762. Parts of this material were presented at ISIT 2001 [6] and WCC 2001 [7].

a given m-covering radius t. We denote by $K^{m,C'}(n,t)$ the size of the smallest subcode of C' with m-covering radius at most t.

Elementary bounds can be obtain by generalizing the sphere bound and by finding certain extremal sets [6].

Theorem 2: (Klapper [6]) Suppose $C \subseteq C'$ are codes with C' linear, and m is a positive integer.

1) Let $T = |\{v \in C' : \mathrm{wt}(v) \le R_m(C)\}|$. Then
$$\binom{|C'|}{m} \le |C| \binom{T}{m}.$$
2) Let D be a set of m vectors in $\mathbf{F}_2^n$ and let $t \ge 0$. If $R_m(C) \le t$, then $|C| \ge |C'|/|\{c \in C' : \forall u \in D : \mathrm{d}(u,c) \le t\}|$.

For a code C of length n and vector $\mathbf{x} \in \mathbf{F}^n$, let $A_i^C(\mathbf{x}) = \{\mathbf{c} \in C : \mathrm{d}(c,\mathbf{x}) = i\}$ and $\mathcal{A}_i^C(\mathbf{x}) = |A_i^C(\mathbf{x})|$. Zhang showed that we can derive lower bounds for the cardinality of C from a lower bound on a linear combination of the $\mathcal{A}_i^C(\mathbf{x})$ [11]. Specifically, suppose that for every $\mathbf{x} \in \mathbf{F}^n$ we have
$$\lambda_0 \mathcal{A}_0^C(\mathbf{x}) + \lambda_1 \mathcal{A}_1^C(\mathbf{x}) + \cdots + \lambda_n \mathcal{A}_n^C(\mathbf{x}) \ge \beta$$
for real constants $\lambda_0, \cdots, \lambda_n, \beta$. Then
$$|C| \ge \frac{\beta 2^n}{\displaystyle\sum_{i=0}^{n} \lambda_i \binom{n}{i}},$$
provided that the denominator is positive. This fact has been used to derive several useful lower bounds for $K^1(n,t)$. We generalize this result by considering vectors to be concatenations of shorter vectors.

Let $n_1, \cdots, n_r$ be positive integers, and let C be a code of length $n = n_1 + n_2 + \cdots + n_r$. For any vector $\mathbf{x} = \mathbf{x}^1|\mathbf{x}^2|\cdots|\mathbf{x}^r \in \mathbf{F}^n$ with $\mathbf{x}^j \in \mathbf{F}^{n_j}$ for $j = 1, \cdots, r$, let
$$\begin{aligned} A^C_{i_1,\cdots,i_r}(\mathbf{x}) &= \{\mathbf{c} \in C : \mathbf{c} = \mathbf{c}^1|\mathbf{c}^2|\cdots|\mathbf{c}^r, \mathbf{c}^j \in \mathbf{F}^{n_j}, \\ &\quad \mathrm{d}(\mathbf{c}^j, \mathbf{x}^j) = i_j, j = 1, \cdots, r\}. \end{aligned}$$
Also let $\mathcal{A}^C_{i_1,\cdots,i_r}(\mathbf{x}) = |A^C_{i_1,\cdots,i_r}(\mathbf{x})|$. We sometimes write $\mathcal{A}^C_{i_1,\cdots,i_r} = \mathcal{A}^C_{i_1,\cdots,i_r}(0^n)$ for simplicity.

Theorem 3: Let C be a subcode of the linear code C' and let $\lambda_{i_1,\cdots,i_r}, \beta$ be real constants. Suppose that for every $\mathbf{x} \in C'$ we have
$$\sum_{i_1=0}^{n_1} \cdots \sum_{i_r=0}^{n_r} \lambda_{i_1,\cdots,i_r} \mathcal{A}^C_{i_1,\cdots,i_r}(\mathbf{x}) \ge \beta \qquad (2)$$
Then
$$|C| \ge \frac{\beta |C'|}{\sum_{i_1=0}^{n_1} \cdots \sum_{i_r=0}^{n_r} \lambda_{i_1,\cdots,i_r} \mathcal{A}^{C'}_{i_1,\cdots,i_r}},$$
provided that the denominator is positive. Similarly, suppose that equation (2) holds for every $\mathbf{x} \notin C'$. Then
$$|C| \ge \frac{\beta(2^n - |C'|)}{\sum_{i_1=0}^{n_1} \cdots \sum_{i_r=0}^{n_r} \lambda_{i_1,\cdots,i_r} (\binom{n}{i} - \mathcal{A}^{C'}_{i_1,\cdots,i_r})},$$
provided that the denominator is positive.

Proof: For every $i_1, \cdots, i_r$ we have
$$\begin{aligned} \sum_{\mathbf{x} \in C'} \mathcal{A}^C_{i_1,\cdots,i_r}(\mathbf{x}) &= |\{(\mathbf{c}, \mathbf{x}) : \mathbf{c} = \mathbf{c}^1|\cdots|\mathbf{c}^r \in C, \\ &\quad \mathbf{x} = \mathbf{x}^1|\cdots|\mathbf{x}^r \in C', \mathrm{d}(\mathbf{c}^j, \mathbf{x}^j) = i_j, \\ &\quad j = 1, \cdots, r\}| \\ &= \sum_{\mathbf{c} \in C} \mathcal{A}^{C'}_{i_1,\cdots,i_r}(\mathbf{c})| \\ &= |C| \mathcal{A}^{C'}_{i_1,\cdots,i_r}. \end{aligned}$$
Thus summing the inequalities (2) over all $\mathbf{x} \in \mathbf{F}^n$ gives the desired inequality. □

Corollary 1: If every subcode of C' with m-covering radius at most t satisfies equation (2) for every $\mathbf{x} \in C'$, then
$$K^{m,C'}(n,t) \ge \frac{\beta |C'|}{\sum_{i_1=0}^{n_1} \cdots \sum_{i_r=0}^{n_r} \lambda_{i_1,\cdots,i_r} \mathcal{A}^{C'}_{i_1,\cdots,i_r}}.$$
If every subcode of C' with m-covering radius at most t satisfies equation (2) for every $\mathbf{x} \notin C'$, then
$$K^{m,C'}(n,t) \ge \frac{\beta(2^n - |C'|)}{\sum_{i_1=0}^{n_1} \cdots \sum_{i_r=0}^{n_r} \lambda_{i_1,\cdots,i_r} (\binom{n}{i} - \mathcal{A}^{C'}_{i_1,\cdots,i_r})}.$$
We can use linear inequalities to obtain bounds for $K^m(n,t)$ in terms of $K^r(n,t)$ for $r \le m-2$.

Theorem 4: If $t \ge n/2$ and $m \ge 3$ then
$$K^{m,C'}(n,t) \ge \frac{|C'|}{\sum_{i=n-t}^{t} \mathcal{A}_i^{C'}} K^{m-2,C'}(n,t)$$
and
$$K^{m,C'}(n,t) \ge \frac{2^n - |C'|}{\sum_{i=n-t}^{t} (\binom{n}{i} - \mathcal{A}_i^{C'})} K^{m-2,C'}(n,t)$$
Proof: Suppose that $C \subseteq C'$ is a code with $R_m(C) = t$. For every $\mathbf{x}$ let $C_{\mathbf{x}} = \{\mathbf{c} \in C : n - t \le \mathrm{d}(\mathbf{x}, \mathbf{c}) \le t\}$. Suppose $\mathbf{y}_1, \cdots, \mathbf{y}_{m-2} \in \mathbf{F}^n$. Then there exists a $\mathbf{c} \in C$ such that $\mathrm{d}(\mathbf{c}, \mathbf{y}_i) \le t$ for $i = 1, \cdots, m-2$, $\mathrm{d}(\mathbf{c}, \mathbf{x}) \le t$, and $\mathrm{d}(\mathbf{c}, \overline{\mathbf{x}}) \le t$. It follows that $\mathbf{c} \in C_{\mathbf{x}}$. Thus $R_{m-2}(C_{\mathbf{x}}) \le t$, so $|C_{\mathbf{x}}| \ge K^{m-2,C'}(n,t)$. This implies the linear inequality
$$\sum_{i=n-t}^{t} \mathcal{A}_i^C(\mathbf{x}) \ge K^{m-2,C'}(n,t)$$
and we can apply either part of Theorem 3. □

III. General Bounds

In this section we use linear inequalities to improve the bounds arising from an earlier construction [5]. Suppose H is an $s \times s$ matrix each of whose entries is one or minus one. Let $\mathbf{v}_1, \mathbf{v}_2, \cdots \mathbf{v}_s$ be the rows of H with $\mathbf{v}_i = (v_{i,1}, \cdots, v_{i,s})$. Let $k > 0$ and $n = ks$. We construct a set D of $m = 2s$ vectors and obtain bounds on the sizes of codes with given m-covering radii. Define $\phi : \{\pm 1\} \to \{0, 1\}$ by $\phi(1) = 0$ and $\phi(-1) = 1$. For each $i = 1, \cdots, s$, let
$$\mathbf{u}_i = \phi(v_{i,1})^k | \cdots | \phi(v_{i,s})^k.$$
We set $D = \{\mathbf{u}_i, \overline{\mathbf{u}_i} : i = 1, \cdots, s\}$. We have $m \ge 2$, so we let $t \ge n/2$. Let $\mathbf{c} = \mathbf{c}^1|\cdots|\mathbf{c}^s$ be any codeword, with each

$\mathbf{c}^j$ of length $n_j = k$ and weight d_j. The distance from $\mathbf{c}$ to $\mathbf{u}_i$ is

$$\sum_{v_{i,j}=1} d_j + \sum_{v_{i,j}=-1} (k - d_j) = \sum_{j=1}^{s} v_{i,j} d_j + k|\{j : v_{i,j} = -1\}|.$$

Thus $\mathbf{u}_i$ and $\overline{\mathbf{u}_i}$ are both within distance t of $\mathbf{c}$ if

$$n - t \le \sum_{j=1}^{s} v_{i,j} d_j + k|\{j : v_{i,j} = -1\}| \le t. \tag{3}$$

Let Δ_i be the set of multi-indices $\delta = (d_1, \cdots, d_s)$ satisfying equation (3). Then for any $\mathbf{x}$, the condition that $\mathbf{x} + D$ is covered by a codeword within radius t says that

$$\bigcap_{i=1}^{s} \bigcup_{(d_1,\cdots,d_s)\in\Delta_i} A^C_{d_1,\cdots,d_s}(\mathbf{x}) \ne \emptyset.$$

Thus

$$\begin{aligned} \bigcap_{i=1}^{s} \bigcup_{(d_1,\cdots,d_s)\in\Delta_i} A^C_{d_1,\cdots,d_s}(\mathbf{x}) = \\ \bigcup_{(d_1,\cdots,d_s)\in\bigcap_{i=1}^{s}\Delta_i} A^C_{d_1,\cdots,d_s}(\mathbf{x}) \\ \ne \quad \emptyset. \end{aligned}$$

Thus

$$\sum_{(d_1,\cdots,d_s)\in\Delta} \mathcal{A}^C_{d_1,\cdots,d_s}(\mathbf{x}) \ge 1,$$

where $\Delta = \bigcap_{i=1}^{s} \Delta_i$. By Theorem 3, the following theorem holds.

Theorem 5: For any n, s and matrix H as above, if s divides n then

$$K^{2s}(n,t) \ge \frac{2^n}{\displaystyle\sum_{\substack{(d_1,\cdots,d_s)\\ \in\bigcap_{i=1}^{s}\Delta_i}} \prod_{j=1}^{s} \binom{n/s}{d_j}}.$$

Suppose that $a = t - n/2$ is kept constant. Then all the binomial coefficients in Theorem 5 are approximately equal. Since each is at most $\binom{k}{k/2}$, we have the bound

$$K^{2s}(n,t) \ge \frac{2^n}{|\Delta|\binom{n/s}{n/(2s)}^s}.$$

The size of Δ depends on the choice of the matrix H. In fact Δ consists of the intersection of the integer lattice $\mathbf{Z}^s$ with the set B of points $\mathbf{x} = (x_1, \cdots, x_s)$ with real coordinates such that

$$n - t \le \sum_{j=1}^{s} v_{i,j} x_j + k|\{j : v_{i,j} = -1\}| \le t,$$

for all i. Thus we expect that there are about $\mathrm{volume}(B)$ points in Δ. But HB consists of the set of points $\mathbf{y} = (y_1, \cdots, y_s)$ with real coordinates such that

$$n - t \le y_i + k|\{j : v_{i,j} = -1\}| \le t,$$

for all i, and HB thus has volume $(2n-t)^s$. It follows that B has volume $(2n-t)^s/\det(H)$ and Δ has approximately this many points..

Thus we expect to obtain the best lower bounds by maximizing the determinant of H. The problem of maximizing the determinant of a matrix of plus and minus ones is old and not completely solved [10]. This determinant is maximized at $s^{s/2}$ if there exists a Hadamard matrix of order s. For this it is necessary (and it is conjectured that it is sufficient) that s be divisible by 4. In other cases the maximum is a constant (less than one) multiple of $s^{s/2}$. Thus in general we can say that the determinant of H is of the form $cs^{s/2}$ with $0 < c \le 1$. Thus our bound becomes

$$K^{2s}(n,t) \ge \frac{cs^{s/2}2^n}{(2t-n)^s\binom{n/s}{n/(2s)}^s} \sim \frac{c\pi^{s/2}n^{s/2}}{2^{s/2}(2t-n)^s}$$

by Stirling's formula.

In particular, the bound is asymptotically $\Omega(n^{s/2})$ for fixed s. If $s \le 2$, so $m = 2s \le 4$, this bound by itself is weaker than one obtained in §IV using quite different methods. However, we show that the two methods can be combined to obtain improved bounds for $m \ge 4$.

IV. Bounds from Balancing Sets

If n is a positive integer, then a set S in $R = \{\pm 1\}^n$ is called a *balancing set* of order $d \ge 0$ if for every $\mathbf{a} \in R$ there is a vector $\mathbf{b} \in S$ such that $-d \le \mathbf{a} \cdot \mathbf{b} \le d$. Here $\mathbf{a} \cdot \mathbf{b}$ denotes the usual dot product of real vectors. Alon, Bergmann, Coppersmith, and Odlyzko determined the carinality of the smallest balancing set [1].

Theorem 6: (Alon, Bergmann, Coppersmith, and Odlyzko [1]) For every n, the smallest balancing set of order d has $\lceil n/(d+1) \rceil$ elements.

The size of the smallest balancing set is related to $K^2(n,t)$. For $\mathbf{x} \in \mathbf{F}^n$, let $\psi(\mathbf{x})$ be the same vector with 0 replaced by 1 and 1 replaced by -1. Then for $\mathbf{x} = (x_1 \cdots, x_n), \mathbf{y} = (y_1 \cdots, y_n) \in \mathbf{F}^n$, we have

$$\begin{aligned} \psi(\mathbf{x}) \cdot \psi(\mathbf{y}) &= |\{i : x_i = y_i\}| - |\{i : x_i \ne y_i\}| \\ &= n - 2|\{i : x_i \ne y_i\}| \\ &= n - 2\mathrm{d}(\mathbf{x}, \mathbf{y}). \end{aligned}$$

Thus $n - 2t \le \psi(\mathbf{x}) \cdot \psi(\mathbf{y}) \le 2t - n$ if and only if $n - t \le \mathrm{d}(\mathbf{x}, \mathbf{y}) \le t$. This pair of inequalities holds if and only if both $\mathbf{x}$ and its complement are contained in a ball of radius t centered at $\mathbf{y}$. Thus the size of the smallest balancing set of order $2t - n$ is a lower bound for $K^2(n,t)$.

We can also obtain an upper bound. Let $t \ge n/2$ and let C be a code whose image under ψ is a balancing set of order $2t - n$. Let $\mathbf{x} \in \mathbf{F}^n$. Then there is a $\mathbf{c} \in C$ with $n - t \le \mathrm{d}(\mathbf{c}, \mathbf{x}) \le t$. Note that the same pair of inequalities holds with $\mathbf{c}$ replaced by its bitwise complement. Now let $\mathbf{y} \in \mathbf{F}^n$ be another vector. Then either $\mathrm{d}(\mathbf{c}, \mathbf{y}) \le n/2$ or $\mathrm{d}(\overline{\mathbf{c}}, \mathbf{y}) \le n/2$. Thus the pair $\mathbf{x}, \mathbf{y}$ is covered by some vector in $C \cup C'$, where C' is the set of bitwise complements of vectors in C. This proves the following theorem.

Theorem 7: For every n and $t \ge n/2$ we have

$$\left\lceil \frac{n}{2t-n+1} \right\rceil \le K^2(n,t) \le 2\left\lceil \frac{n}{2t-n+1} \right\rceil.$$

Combining this with Theorem 4 we have the following.

Corollary 2: If m is even then

$$\begin{aligned} K^m(n,t) &\ge K^2(n,t)\left(\frac{2^n}{\sum\limits_{i=n-t}^{t}\binom{n}{i}}\right)^{(m-2)/2} \\ &\ge \left\lceil\frac{n}{2t-n+1}\right\rceil\left(\frac{2^n}{\sum\limits_{i=n-t}^{t}\binom{n}{i}}\right)^{(m-2)/2} . \end{aligned}$$

We can make the (crude if t is large) estimate

$$\binom{n}{i} \le \binom{n}{n/2} \sim 2^n\left(\frac{2}{\pi n}\right)^{1/2}.$$

Thus we have

$$K^m(n,t) \ge \left(\frac{(\pi n/2)^{(m-2)/4}}{(2t-n+1)^{m/2}}\right)n.$$

If we keep $t - n/2$ constant and let n grow, then this is asymptotically $K^m(n,t) \in \Omega(n^{(m+2)/4})$. If m is constant, this asymptotically exceeds the bound in Theorem 1 by a factor of $n^{1/2}$.

For larger m we combine this approach with the method of §III. Again let C be a length n code with $R_m(C) \le t$. As in §III, let H be an $s \times s$ matrix each of whose entries is one or minus one. Now, however, we assume $2s \le m-2$. Construct D as before, so $|D| = 2s$. Let $\mathbf{x} \in \mathbf{F}^n$ be any vector and let $C_{\mathbf{x}} = \{c \in C : \forall u \in D : \mathrm{d}(c, u+x) \le t\}$. Then $R_{m-2s}(C_{\mathbf{x}}) \le t$, so $|C_{\mathbf{x}}| \ge K^{m-2s}(n,t)$. If Δ is as in §III, then

$$\sum_{(d_1,\cdots,d_s)\in\Delta} \mathcal{A}^C_{d_1,\cdots,d_s}(\mathbf{x}) \ge K^{m-2s}(n,t). \tag{4}$$

This implies the following theorem.

Theorem 8: If Δ is as above, then

$$K^m(n,t) \ge \frac{2^n}{\sum\limits_{\substack{(d_1,\cdots,d_s)\\ \in\Delta}}\prod\limits_{j=1}^{s}\binom{k}{d_j}}K^{m-2s}(n,t).$$

We can iterate this and obtain lower bounds for $K^m(n,t)$ in terms of $K^{m'}(n,t)$ for small m'. At each iteration we may make various choices for s as long as the sum of the choices is at most $(m-1)/2$. The question of which sequence of choices leads to the optimal (i.e., maximal) lower bound amounts to asking for the maximal product of terms of the form

$$\frac{2^n}{\sum\limits_{\substack{(d_1,\cdots,d_s)\\ \in\Delta}}\prod\limits_{j=1}^{s}\binom{k}{d_j}}$$

over a set of pairs (s, H) with the sum of the ss fixed. This is a complicated question.

V. Examples

In this section we demonstrate the techniques described in this paper by finding bounds on the sizes of subcodes of a code C' whose codimension is 1. Let E^r denote the set of even weight vectors of length r. Let $C' = E^k \times \mathbf{F}^r$ and let $n = k + r$ with $k \ge 1$. That is, C' has a single parity check of weight k. Then C' has minimum distance 1 if $r \ge 1$ and minimum distance 2 if $r = 0$. Its ordinary covering radius is 1: if $\mathbf{x} = \mathbf{x}^1|\mathbf{x}^2 \in \mathbf{F}^n$ with $\mathbf{x}^1 \in \mathbf{F}^k$ and $\mathbf{x}^2 \in \mathbf{F}^r$, then we can find $\mathbf{c}^1 \in E^k$ so that $\mathrm{d}(\mathbf{c}^1, \mathbf{x}^1) \le 1$. Then $\mathbf{c}^1|\mathbf{x}^2 \in C'$ and $\mathrm{d}(\mathbf{c}^1|\mathbf{x}^2, \mathbf{x}) \le 1$.

Suppose that C is a subcode of C' and the 1-covering radius of C is 1. Using an improvement to the sphere bound [2] we get that

$$|C| \ge \begin{cases} 2^n/(1+n) & \text{if } n \text{ is odd} \\ 2^n/n & \text{if } n \text{ is even.} \end{cases} \tag{5}$$

We can do better by noting that every vector $\mathbf{x} = \mathbf{x}^1|\mathbf{x}^2 \in C'$ with $\mathbf{x} \in \mathbf{F}^k$ and $\mathbf{x}^2 \in \mathbf{F}^r$ has distance at most 1 from some vector in C of the form $\mathbf{x}^1|\mathbf{y}^2$. It follows that the set $C_{\mathbf{x}^1} = \{\mathbf{y}^2 : \mathbf{x}^1|\mathbf{y}^2 \in C\}$ is a code of length r and covering radius 1. Hence

$$|C_{\mathbf{x}^1}| \ge \begin{cases} 2^r/(1+r) & \text{if } r \text{ is odd} \\ 2^r/r & \text{if } r \text{ is even.} \end{cases}$$

Therefore

$$|C| \ge \begin{cases} 2^{n-1}/(1+r) & \text{if } r \text{ is odd} \\ 2^{n-1}/r & \text{if } r \text{ is even.} \end{cases} \tag{6}$$

(The weaker bound that we would get by ignoring parities can be obtained from linear inequalities as well.) This improves on equation (5) if r is less than approximately $n/2$ (there are various cases depending on the parities of n and r).

On the other hand, if $\mathbf{x} \in \mathbf{F}^n$, then there is a codeword $\mathbf{c} \in C$ with $\mathrm{d}(\mathbf{c}, \mathbf{x}) \le 1$. Thus

$$\mathcal{A}^C_0(\mathbf{x}) + \mathcal{A}^C_1(\mathbf{x}) \ge 1. \tag{7}$$

By the second part of Theorem 3, we have

$$|C| \ge \frac{2^{n-1}}{k},$$

which improves on equations (5) and (6) when k is less than about $n/2$. It follows that any code that has covering radius 1 and has size close to $2^n/n$ cannot have a parity check of either low or high weight.

Now suppose that C is a subcode of C' whose 1-covering radius is 2. If $\mathbf{x} \in \mathbf{F}^n$, then there is a codeword $\mathbf{c} \in C$ whose distance from $\mathbf{x}$ is at most 2. Thus

$$\mathcal{A}^C_0(\mathbf{x}) + \mathcal{A}^C_1(\mathbf{x}) + \mathcal{A}^C_2(\mathbf{x}) \ge 1. \tag{8}$$

If we ignore the fact that C is a subcode of C', we get the bound

$$|C| \ge \frac{2^{n+1}}{n^2+n+2}. \tag{9}$$

Again, there are various other slight improvements known in some cases of n. We can also think of C as a subcode of C'. We have

$$\mathcal{A}^{C'}_2(\mathbf{x}) = \binom{r}{2} + \binom{k}{2} \tag{10}$$

if $\mathbf{x} \in C'$. Using Theorem 3, this leads to the bounds

$$|C| \geq \frac{2^{n-1}}{1+r+\binom{r}{2}+\binom{k}{2}} = \frac{2^n}{2k^2-2(n+1)k+n^2+n+2} \tag{11}$$

and

$$|C| \geq \frac{2^{n-1}}{k(r+1)} = \frac{2^{n-1}}{k(n-k+1)}. \tag{12}$$

Equation(11) improves on equation (9) when $(n+1-\sqrt{n-1})/2 < k < (n+1+\sqrt{n-1})/2$, while equation (12) improves on equation (9) when $k < (n+1-\sqrt{n-1})/2$ or $k > (n+1+\sqrt{n-1})/2$. It follows that any code with minimal size for codes with covering radius 2 can only have parity checks with weight close to $(n+1 \pm \sqrt{n-1})/2$.

Next we consider the m-covering radii of a subcode C of C' for larger m. For $m=2$, the bounds we can obtain on the size of C by the techniques of §II are still weaker than those obtained from §IV by ignoring C'. In fact we have

$$K^{2,C'}(n,t) \leq K^2(n,t+1) \leq 2\left\lceil \frac{n}{2t-n+3} \right\rceil,$$

for any $t \geq \lceil n/2 \rceil + 1$, since the 1-covering radius of C' is 1. Thus we consider the cases $m=4$ and $m=6$.

First we find $R_4(C')$, and $R_6(C')$. Recall that by Corollary 1 of [4], for any $m \geq 1$,

$$R_m(E^k) = 1 + R_m(\mathbf{F}^{k-1}). \tag{13}$$

Thus

$$R_m(C') \leq 1 + R_m(\mathbf{F}^{k-1}) + R_m(\mathbf{F}^r). \tag{14}$$

Moreover, the 1-covering radius of C' is 1, so for any m,

$$R_m(C') \leq 1 + R_m(\mathbf{F}^n). \tag{15}$$

Also, if O^k is the set of odd weight vectors of length k, then $R_m(O^k \times \mathbf{F}^r) = R_m(E^k \times \mathbf{F}^r)$.

Theorem 9: Let $n \geq 2$. If n is even, then $R_4(C') = n/2+1$. If $k=0$ and r is odd, then $R_4(C') = (n+1)/2$. If $k>0$ is even and r is odd, then $R_4(C') = (n+3)/2$. If k is odd and $r=0$ or if $k=1$ and r is even, then $R_4(C') = (n+3)/2$. If $k \geq 3$ is odd and $r \geq 2$ is even, then $R_4(C') = (n+1)/2$.

Proof: The case when $k=0$ follows from [4] since then $C' = \mathbf{F}^n$. So assume $k>0$. It follows from [4] that $R_4(C') \geq R_2(E^k) + R_2(\mathbf{F}^r) = 1 + \lceil (k-1)/2 \rceil + \lceil r/2 \rceil$.

For any set of 4 vectors of length at least 4 there is a pair of coordinates in which only 3 distinct binary pairs occur. Let $n \geq 4$, and let $\mathbf{x}_1, \cdots, \mathbf{x}_4$ be vectors of length n. Suppose that only 3 binary pairs occur in coordinates i and j. Let k' be k minus the number of i and j that are less than or equal to k, and let r' be r minus the number that are greater than k. For any vector $\mathbf{y}$, let $\mathbf{y}'$ be the length 2 vector consisting of the ith and jth coordinates of $\mathbf{y}$, and let $\mathbf{y}''$ be the remaining coordinates. Let $\mathbf{c}^0$ be a vector of length 2 with $\mathrm{d}(\mathbf{c}^0, \mathbf{x}'_\ell) \leq 1$. If the weight of the part of $\mathbf{c}^0$ that lies among the first k coordinates of C' is even, let $C'' = E^{k'} \times \mathbf{F}^{r'}$. Otherwise let $C'' = O^{k'} \times \mathbf{F}^{r'}$. In either case, $R_4(C'') = R_4(E^{k'} \times \mathbf{F}^{r'})$. Let $\mathbf{c}^1 \in C$" have distance at most $R_4(E^{k'} \times \mathbf{F}^{r'})$ from every $\mathbf{x}''_\ell$, and let $\mathbf{c}$ be the vector with $\mathbf{c}' = \mathbf{c}^0$ and $\mathbf{c}'' = \mathbf{c}^1$. Then $\mathbf{c}$ has distance at most $1 + R_4(E^{k'} \times \mathbf{F}^{r'})$ from every $\mathbf{x}_\ell$. It follows that

$$R_4(E^k \times \mathbf{F}^r) \leq 1 + R_4(E^{k'} \times \mathbf{F}^{r'}).$$

Let n be even. Repeating this eventually reduces to one of the cases $(k,r) = (2,0)$, $(1,1)$, or $(0,2)$. The 4-covering radius in each of these cases is 2. Thus the original 4-tuple of n-vectors can be covered in radius $(n-2)/2 + R_4(E^1 \times \mathbf{F}^1) = n/2+1$ by C'. This upper bound equals the lower bound.

Similarly, when k is even and r is odd we can reduce to one of the cases $(k,r) = (2,3)$ or $(2,1)$ and do a similar analysis.

Now let k be odd and r be even. If $k \geq 3$ and $r \geq 2$, then the series of reductions can be arranged to end with $E^3 \times \mathbf{F}^2$, which has 4-covering radius equal to 3. This gives $R_4(C') \leq (n+1)/2$. If $r=0$, then $C' = E^n$ and $R_4(C') = (n+3)/2$ follows from $R_4(C') = 1 + R_4(\mathbf{F}^{n-1})$ and previous work [4]. Finally, let $k=1$. Then either $\{10^r, 10^{r/2}1^{r/2}, 1^{1+r/2}0^{r/2}, 1^{r+1}\}$ (if $r \equiv 2 \bmod 4$) or $\{10^r, 10^{r/2-1}1^{r/2+1}, 1^{r/2}0^{r/2+1}, 1^{r+1}\}$ (if $r \equiv 0 \bmod 4$) cannot be covered by C' in radius $(n+1)/2$. □

Theorem 10: If n is even, then $n/2+1 \leq R_6(C') \leq n/2+2$. If k is even and r is odd, then $R_6(C') = (n+3)/2$. If k is odd and r is even, then $(n+1)/2 \leq R_6(C') \leq (n+3)/2$.

Proof: The upper bounds follows from equation (14) and [3]. The lower bounds follows from the fact that $R_6(C') \geq R_3(E^k) + R_2(\mathbf{F}^r)$. In theory we could use the same reduction approach as for the 4-covering radius, but in practice the base case is infeasible. □

Now we return to bounding $K^{4,C'}(n,t)$ and $K^{6,C'}(n,t)$. As usual we are most interested in codes with minimal covering radii. Let n be even, $C \subset C'$, and suppose that $R_4(C) = t = n/2+1$. Ignoring C', the bound we obtain from Corollary 2 is

$$\begin{aligned} |C| \quad &\geq \quad \frac{2^n}{\binom{n}{\frac{n}{2}-1}+\binom{n}{\frac{n}{2}}+\binom{n}{\frac{n}{2}+1}} K^2(n,\frac{n+1}{2}) \qquad (16) \\ &\sim \quad \frac{\pi^{1/2}n^{1/2}}{2^{3/2}} K^2(n,n/2+1). \end{aligned}$$

We can also think of C as a subcode of C'. If we constrain the vector $\mathbf{x}$ in equation (4) to be in C', then we obtain the perhaps better inequality

$$\sum_{(d_1,\cdots,d_s)\in\Delta} \mathcal{A}^C_{d_1,\cdots,d_s}(\mathbf{x}) \geq K^{m-2s,C'}(n,t). \tag{17}$$

In the current case this leads to the bounds

$$|C| \geq \frac{2^{n-1}}{\mathcal{A}^{C'}_{n/2-1}+\mathcal{A}^{C'}_{n/2}+\mathcal{A}^{C'}_{n/2+1}} K^{2,C'}(n,n/2+1) \tag{18}$$

and

$$|C| \geq \frac{2^{n-1}K^{2,C'}(n,n/2+1)}{\binom{n}{n/2}+2\binom{n}{n/2+1}-\mathcal{A}^{C'}_{n/2-1}-\mathcal{A}^{C'}_{n/2}-\mathcal{A}^{C'}_{n/2+1}}. \tag{19}$$

For example, when $n=6$, the bound in equation (16) is $1.28K^2(n,n/2+1)$. If $k=2$, then the bound in equation (18) is $1.45K^{2,C'}(n,n/2+1)$ and the bound in equation (19) is $1.14K^{2,C'}(n,n/2+1)$. However, if $k=4$, then the bound in equation (18) is $1.23K^{2,C'}(n,n/2+1)$ and the bound in equation (19) is $1.33K^{2,C'}(n,n/2{+}1)$. One of the new bounds is no worse than the bound in equation (16).

Now we consider subcodes of C' whose 6-covering radii are minimal. For simplicity we let n be even and $k = n/2$. Suppose $C \subseteq C'$ and $R_6(C) = n/2{+}1$. Whenever we prove a bound $|C_0| > dK^2(n,t)$ or $|C_0| > dK^{2,C'}(n,t)$ for a subcode $C_0 \subseteq C'$ whose 4-covering radius is t by any of the methods above, we also have a bound $|C| \geq d^2K^2(n,t)$ or $|C| \geq d^2K^{2,C'}(n,t)$.

We can also obtain a bound more directly. Let $D = \{0^n, 1^n, 0^k1^k, 1^k0^k\}$. For any $\mathbf{x}$, $\mathbf{y}$, and $\mathbf{z}$, there is a $\mathbf{c} \in C$ with $\mathrm{d}(\mathbf{c},\mathbf{w}) \leq n/2+1$ for all $\mathbf{w} \in (\mathbf{x}+D) \cup \{\mathbf{y},\mathbf{z}\}$. Let $C_{\mathbf{x}}$ be the set of $\mathbf{c} \in C$ such that $\mathrm{d}(\mathbf{c},\mathbf{w}) \leq n/2+1$ for all $\mathbf{w} \in \mathbf{x}+D$. Then $R_2(C_{\mathbf{x}}) \leq n/2+1$ and $C_{\mathbf{x}} \subseteq C'$, so $|C_{\mathbf{x}}| \geq K^{2,C'}(n,n/2+1)$. We can sum this inequality over all $\mathbf{x} \in \mathbf{F}^n$, $\mathbf{x} \in C'$, or $\mathbf{x} \notin C'$.

To obtain bounds on $|C|$, in each case we must determine what weights of codewords can occur in $C_{\mathbf{x}}$. This depends on various numeric properties of k. For example, suppose $k \equiv 0 \bmod 4$. If $\mathbf{x} \in C'$, then $(i,j) \in \{(k/2,k/2-1),(k/2,k/2),(k/2,k/2+1)\}$. If $\mathbf{x} \notin C'$, then $(i,j) \in \{(k/2+1,k/2),(k/2+1,k/2)\}$. The latter gives the larger bound from Theorem 3,

$$|C| \geq \frac{2^{n-1}}{2\binom{k}{\frac{k}{2}}\binom{k}{\frac{k}{2}-1}} K^{2,C'}(n,k+1).$$

Similar calculations can be made in the other cases.

VI. Conclusions

We have given a strong upper bound for the case $m = 2$, so we now know $K^2(n,t)$ within a factor of 2. For larger m, however, we only know lower bounds on $K^m(n,t)$. These bounds are asymptotically $\Omega(n^{(m+2)/4})$ when $t - n/2$ is fixed, and we conjecture that in fact, $K^m(n,t)$ is $\Theta(n^{(m+2)/4})$ when $t - n/2$ is fixed.

We have also extended these techniques to the problem of finding lower bounds on the size of the smallest subcode of a given linear code with a given m-covering radius. Even when $m = 1$ this is a new question. Perhaps the most surprising result here is that we obtain constraints on optimal codes with small covering radius – they can only have parity checks of restricted types.

There are many refinements of techniques related to the method of linear inequalities that have been used to obtain bounds for codes with small ordinary covering radius [2], [8]. It is possible that these refinements will further improve the results in this paper.

Acknowledgements

The author thanks the refrees for several useful comments that improved this paper.

References

[1] N. Alon, E. Bergmann, D. Coppersmith, and A. Odlyzko, "Balancing Sets of Vectors," *IEEE Trans. Info. Theory*, vol. 34, pp. 128-130, 1988.

[2] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering Codes*. Amsterdam: North-Holland, 1997.

[3] I. Honkala and A. Klapper, "Multicovering Bounds from Relative Covering Radii," to appear, *SIAM Journal on Discrete Math*.

[4] A. Klapper, "The multicovering radii of codes," *IEEE Trans. Info. Theory*, vol. 43, pp. 1372-1377, 1997.

[5] A. Klapper, "Improved Lower Bounds for Multicovering Codes," *IEEE Trans. Info. Theory*, vol. 45, pp. 2532-2534, 1999.

[6] A. Klapper, "Multicovering Bounds from Supercodes," *International Symposium on Information Theory (ISIT) 2001*.

[7] A. Klapper, "Multicovering Bounds from Linear Inequalities," *Workshop on Codes and Cryptography (WCC) 2001*, Paris, January, 2001.

[8] D. Li and W. Chen, "New lower bounds for binary covering codes," *IEEE Trans. Info. Theory*, vol. 40, pp. 1122-1129, 1994.

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

[10] C. Koukouvinos, M. Mitrouli and J. Seberry, "Bounds on the maximum determinant for $(1,-1)$ matrices," *Bull. ICA*, vol. 29, pp. 39-48, 2000.

[11] Z. Zhang, "Linear inequalities for covering codes: Part I – pair covering inequalities," *IEEE Trans. Info. Theory*, vol. 37, pp. 573-582, 1991.

Andrew Klapper received the A.B. degree in mathematics from New York University, New York, NY, in 1974, the M.S. degree in applied mathematics from SUNY at Binghamton, Binghamton, NY, in 1975, the M.S. degree in mathematics from Stanford University, Stanford, CA, in 1976, and the Ph.D. degree in mathematics from Brown University, Providence, RI, in 1982. His thesis, in the area of arithmetic geometry, concerned the existence of canonical subgroups in formal grouplaws.

From 1981 to 1984 he was a Postdoc in the Department of Mathematics and Computer Science at Clark University. From 1984 to 1991 he was an Assistant Professor in the College of Computer Science at Northeastern University. From 1991 to 1993 he was an Assistant Professor in the Computer Science Department at the University of Manitoba. Currently he is a Professor in the Department of Computer Science at the University of Kentucky. He was awarded a University Research Professorship for 2002-03. His past research has included work on algebraic geometry over p-adic integer rings, computational geometry, modeling distributed systems, structural complexity theory, and cryptography. His current interests include statistical properties of pseudo-random sequences with applications in cryptography and CDMA; covering properties of codes; and morris dancing.

Dr. Klapper is a member of the IEEE Information Theory Society and the International Association for Cryptologic Research. He was the general chair of the Crypto '98 conference and was been the Associate for Sequences for the IEEE Transactions on Information Theory from 1999 until 2002.