Further Results on the Covering Radius of Codes

GERARD D. COHEN, MEMBER, IEEE, ANTOINE C. LOBSTEIN, AND N. J. A. SLOANE, FELLOW, IEEE

Abstract—A number of upper and lower bounds are obtained for $K(n, R)$, the minimal number of codewords in any binary code of length n and covering radius R. Several new constructions are used to derive the upper bounds, including an amalgamated direct sum construction for nonlinear codes. This construction works best when applied to normal codes, and we give some new and stronger conditions which imply that a linear code is normal. An upper bound is given for the density of a covering code over any alphabet, and it is shown that $K(n+2, R+1) \leq K(n, R)$ holds for sufficiently large n.

I. Introduction

THE COVERING radius of binary *linear* codes has been extensively studied (see for example [5] and [10]). The present paper is mostly devoted to the covering radius of binary *nonlinear* codes, although we also include some results for linear codes and nonbinary codes.

The study of nonlinear covering codes began around the same time as the study of error-correcting codes, in the work of Taussky and Todd [30], [31], Mattioli [21], Mauldon [22], and Zaremba [35], [36]. Further results were obtained by Kalbfleisch, Stanton, and various coauthors in a series of papers [12], [13], [26]–[29], and by others [7], [18]. This work mostly dealt with codes of covering radius 1 over various alphabets and was independent of the early work on the covering radius of linear codes described in [5]. Several papers have treated linear or nonlinear *ternary* codes of covering radius 1, the so-called football pool problem (see for example [8], [14], [26], and [33]).

Summary of Results

Let $K(n, R)$ denote the minimal number of codewords in any binary (linear or nonlinear) code C of length n and covering radius R. In Section II we give a number of lower bounds on $K(n, R)$ which improve on the sphere bound. Theorems 1 and 2 are lower bounds that are based on finding an *error-correcting* code embedded in C. Section II-B introduces the notion of a *balanced* code and shows that good covering codes cannot be too unbalanced (Theorems 3–5). An inductive argument then shows that $K(2R+2, R) \geq 4$ and $K(2R+3, R) \geq 7$ (Theorems 7 and 8). In Section II-C we study the inequalities that a covering code must satisfy, and we give a general linear programming bound (Theorem 9). Theorem 10 establishes the particular values $K(8,2) \geq 9$, $K(9,2) \geq 13$, and $K(10,3) \geq 8$.

Section III deals with upper bounds on $K(n, R)$. In Section III-A we introduce the notion of a *piecewise constant* code and thus construct codes which show that $K(5,1) = 7$, $K(6,1) = 12$, $K(2R+3, R) = 7$, $K(2R+4, R) \leq 12$, and $K(11,1) \leq 192$.

The concept of a *normal* linear code was introduced in [10], and in Section III-B we extend this to nonlinear codes and define the corresponding amalgamated direct sum (ADS) construction (see Theorem 11). This leads to a number of new codes, proving that $K(11,2) \leq 56$, $K(12,2) \leq 96$, etc.

Two other constructions are described in Sections III-C and -D. The former starts with a code that has the so-called *partitioning property*, and in some cases provides an alternative to the ADS construction (Theorem 12). Section III-D describes a variation on the $|u|u+v|$ construction that is effective for codes with $R = 1$ (Theorem 13). Section III-E gives a brief summary of the results on $K(n, R)$, and in particular gives a table of $K(n, R)$ for $n \leq 23$, $R \leq 4$ (Table I). The only earlier table we have seen is in [12], for $n \leq 8$ and $R = 1$.

The ADS construction works best when applied to normal codes, and in Section IV we give a series of conditions that imply that certain linear codes are normal, considerably strengthening the results in [10]. The principal result is that a code of length $n \leq 12$, or dimension $k \leq 2$, or minimal distance $d \leq 3$, or covering radius $R \leq 2$, must be normal (Theorem 32).

The final two sections are concerned with the conjecture that, for $R \neq n$,

$$K(n+2, R+1) \leq K(n, R)$$

and certain related conjectures. Theorems 33–35 and Corollary 39 show that the conjecture holds for sufficiently large n. The last section deals with covering codes over arbitrary alphabets and introduces the *density* of a covering. It is shown that for a fixed alphabet size and fixed covering radius, as $n \to \infty$ the density is independent of n (Theorems 36 and 38).

Manuscript received June 20, 1985; revised December 30, 1985.

G. D. Cohen and A. C. Lobstein are with the Ecole Nationale Supérieure des Télécommunications, 46 rue Barrault, 75634 Paris Cedex 13, France.

N. J. A. Sloane is with AT&T Bell Laboratories, Murray Hill, NJ 07974.

IEEE Log Number 8608609.

0018-9448/86/0900-0680$01.00

Certain of these results are in Lobstein's thesis [16] (in particular, Theorems 1, 5, 7, 8, 12, 14, and 33–35). Some of this material was presented at the International Conference on Algebra, Algorithms and Codes in 1984 [6] and was announced in [17].

Notation: An $(n, M)R$ code C is a binary code of length n with M codewords and covering radius R. The covering radius of C is sometimes denoted by $CR(C)$. $d(x, y)$ denotes Hamming distance.

II. Lower Bounds

Let $K(n, R)$ denote the minimal number of codewords in any binary code C of length n and covering radius R. The sphere bound (see for example [5]) states that

$$K(n, R) \geq \frac{2^n}{1 + \binom{n}{1} + \cdots + \binom{n}{R}}. \tag{1}$$

Let $\lambda = (\log_2 K(n, R))/n$ be the rate of C. For fixed $\lambda > 0$, (1) implies

$$\frac{R}{n} \geq H_2^{-1}(1 - \lambda)(1 + o(1)) \tag{2}$$

as $n \to \infty$, where H_2 is the binary entropy function. Goblick showed in 1962 [9] (see also [1], [3], [34]) that (2) is asymptotically correct: there exist linear codes for which

$$\frac{R}{n} \sim H_2^{-1}(1 - \lambda) \text{ as } n \to \infty. \tag{3}$$

So no asymptotic improvement on (1) is possible (for fixed positive rate). But for particular values of n and R it is often possible to improve on (1). The improvements can be roughly divided into four classes: 1) improved counting methods, using an embedded error-correcting code; 2) using induction and the notion of a balanced code; 3) using linear inequalities; and 4) improvements specifically for linear codes. We shall not discuss 4) here but instead refer the reader to [5] and [10] (see for example the proof of Theorem 22 in [10]).

A. Improved Counting Methods, Using an Embedded Error-Correcting Code

We illustrate by giving two theorems that appear to be the most useful. Further generalizations could easily be obtained. Let $A(n, d)$ denote the maximal number of codewords in any binary code of length n and minimal Hamming distance d, with the convention that $A(n, d) = 1$ if $d > n$. A table of $A(n, d)$ for $n \leq 23$, $d \leq 9$ is given in [20, p. 674]. This should be supplemented by the values

$$A(9,3) = 40,\ A(10,3) \leq 79,\ A(11,3) \leq 158,$$
$$A(16,3) \geq 2720,\ A(18,3) \geq 10240,\ A(19,3) \geq 20480,$$
$$A(20,9) \leq 52,\ A(21,9) \leq 89,$$

obtained by Best [2], Romanov [24], and Tietäväinen [32].

Theorem 1:

$$K(n, R) \geq \frac{2^n - A(n, 2R+1)\binom{2R}{R}}{\sum_{i=0}^{R}\binom{n}{i} - \binom{2R}{R}}, \tag{4}$$

provided the denominator is positive.

Proof: Suppose C has covering radius R, and let C_0 be a maximal subcode of C with minimal Hamming distance at least $2R + 1$. (If $2R + 1 > n$, we take C_0 to contain a single codeword.) The spheres of radius R around codewords of C_0 are disjoint, so C_0 covers (i.e., is within distance $\leq R$ of) precisely

$$|C_0|\left(1 + \binom{n}{1} + \cdots + \binom{n}{R}\right) \tag{5}$$

vectors. Let $C_1 = C \setminus C_0$ denote the remaining codewords. For $c_1 \in C_1$, let $\phi(c_1)$ denote the number of vectors in $\mathbb{F}_2^n$ covered by c_1 that are not already covered by C_0. Since C_0 is maximal, there is at least one codeword (c_0 say) in C_0 at distance $\leq 2R$ from c_1. Then $\phi(c_1)$ takes its maximal value when there is just one such c_0, and that c_0 is at distance $2R$ from c_1. When $d(c_0, c_1) = 2R$, there are $\binom{2R}{R}$ vectors at distance R from both c_0 and c_1. Therefore

$$\phi(c_1) \leq \left(1 + \binom{n}{1} + \cdots + \binom{n}{R}\right) - \binom{2R}{R}. \tag{6}$$

Then we have

$$\begin{aligned}
2^n &= \text{total number of vectors covered by } C \\
&\leq |C_0|\left(1 + \binom{n}{1} + \cdots + \binom{n}{R}\right) + \sum_{c_1 \in C_1} \phi(c_1) \\
&\leq |C_0| \sum_{i=0}^{R}\binom{n}{i} + |C_1|\left\{\sum_{i=0}^{R}\binom{n}{i} - \binom{2R}{R}\right\} \\
&= |C_0| \sum_{i=0}^{R}\binom{n}{i} + (|C| - |C_0|)\left\{\sum_{i=0}^{R}\binom{n}{i} - \binom{2R}{R}\right\} \\
&= |C|\left\{\sum_{i=0}^{R}\binom{n}{i} - \binom{2R}{R}\right\} + |C_0|\binom{2R}{R} \\
&\leq |C|\left\{\sum_{i=0}^{R}\binom{n}{i} - \binom{2R}{R}\right\} + A(n, 2R+1)\binom{2R}{R},
\end{aligned}$$

and (4) follows.

Remarks: a) Provided the denominator is positive, (4) is always at least as good as the sphere bound (1). b) If the exact value of $A(n, 2R + 1)$ is not known, an upper bound on it may be used in (4). c) The entries marked b in Table I at the end of Section III were obtained from (4).

Theorem 2:

$$K(n, R) \geq \frac{2^n - 2A(n, 2R+1)\binom{2R}{R}}{\sum_{i=0}^{R}\binom{n}{i} - \frac{3}{2}\binom{2R}{R}}, \tag{7}$$

provided the denominator is positive.

Proof: As in Theorem 1 we first choose a maximal subcode C_0 of minimal Hamming distance $\geq 2R+1$. In $C \setminus C_0$ we choose a second maximal subcode C_1 of minimal Hamming distance $\geq 2R+1$ and let C_2 denote the remaining codewords. Equations (5) and (6) still apply. For $c_2 \in C_2$, let $\phi(c_2)$ denote the number of vectors in $\mathbb{F}_2^n$ covered by c_2 that are not already covered by C_0 or C_1. $\phi(c_2)$ takes its maximal value when there are codewords $c_0 \in C_0, c_1 \in C_1$ in one of the following three configurations:

$$d(c_0,c_2) = d(c_1,c_2) = 2R,\ d(c_0,c_1) = 2$$

$$d(c_0,c_2) = 2R,\ d(c_1,c_2) = 2R-1,\ d(c_0,c_1) = 1$$

$$d(c_0,c_2) = 2R-1,\ d(c_1,c_2) = 2R,\ d(c_0,c_1) = 1.$$

In each case we find

$$\phi(c_2) \leq \sum_{i=0}^{R} \binom{n}{i} - 3\binom{2R-1}{R-1}. \tag{8}$$

Then we have

$$\begin{aligned} 2^n &\leq |C_0| \sum_{i=0}^{R} \binom{n}{i} + |C_1| \left\{ \sum_{i=0}^{R} \binom{n}{i} - \binom{2R}{R} \right\} \\ &\quad + \{|C| - |C_0| - |C_1|\} \left\{ \sum_{i=0}^{R} \binom{n}{i} - 3\binom{2R-1}{R-1} \right\} \\ &= |C| \left\{ \sum_{i=0}^{R} \binom{n}{i} - \frac{3}{2}\binom{2R}{R} \right\} + \frac{1}{2}\{3|C_0| + |C_1|\}\binom{2R}{R} \\ &\leq |C| \left\{ \sum_{i=0}^{R} \binom{n}{i} - \frac{3}{2}\binom{2R}{R} \right\} + 2A(n,2R+1)\binom{2R}{R}, \end{aligned}$$

and (7) follows.

Remarks: a) Neither of (4) or (7) is always better than the other. b) Again an upper bound on $A(n,2R+1)$ may be used if the exact value is unknown. c) The entries marked c in Table I were obtained from (7).

B. Balanced Codes and Induction

A code C containing M codewords is *balanced* if in each coordinate position there are either $[M/2]$ zeros and $[(M+1)/2]$ ones, or $[(M+1)/2]$ zeros and $[M/2]$ ones, where $[x]$ denotes the largest integer less than or equal to x. We conjecture (but cannot prove) that among the codes with $K(n,R)$ codewords there is always one that is balanced.

The next theorem shows that codes cannot be too unbalanced. Let $M_i(a)$ be the number of codewords $(c_1 \cdots c_n) \in C$ with $c_i = a$, and let $M_{ij}(ab)$ be the number of codewords with $c_i = a$ and $c_j = b$ (for $i, j = 1, \cdots, n$; $a, b = 0$ or 1). A code is balanced if, for each i, $M_i(0)$ is either $[M/2]$ or $[(M+1)/2]$.

Theorem 3: Let C have covering radius R and length $n \geq R+1$. Then

$$M_i(a) \geq \frac{2^{n-1} - |C| \sum_{i=0}^{R-1} \binom{n-1}{i}}{\binom{n-1}{R}} \tag{9}$$

for all i and a.

The case $R = 1$ was given in [29].

Proof: Let us consider how the 2^{n-1} vectors with a zero in the ith place are covered. The $M_i(0)$ codewords with $c_i = 0$ each cover

$$1 + \binom{n-1}{1} + \cdots + \binom{n-1}{R}$$

such vectors, and the $M_i(1)$ codewords with $c_i = 1$ each cover

$$1 + \binom{n-1}{1} + \cdots + \binom{n-1}{R-1}.$$

Therefore

$$M_i(0) \sum_{j=0}^{R} \binom{n-1}{j} + M_i(1) \sum_{j=0}^{R-1} \binom{n-1}{j} \geq 2^{n-1}, \tag{10}$$

and

$$M_i(0) + M_i(1) = |C|. \tag{11}$$

Solving for $M_i(0)$ and $M_i(1)$ leads to (9).

There is a similar result for pairs of columns.

Theorem 4:

$$M_{ij}(ab) \geq \frac{2^{n-2} - |C| \sum_{i=0}^{R-2} \binom{n-2}{i} - (M_i(a) + M_j(b))\binom{n-2}{R-1}}{\binom{n-2}{R} - \binom{n-2}{R-1}}, \tag{12}$$

whenever the denominator is positive (and with the usual convention that an empty sum is zero).

Again the case $R = 1$ was given in [29].

Proof: Let us consider how the 2^{n-2} vectors with $x_i = 0$, $x_j = 0$ are covered. Instead of (10) we obtain

$$\begin{aligned} &M_{ij}(00) \sum_{k=0}^{R} \binom{n-2}{k} + (M_{ij}(01) + M_{ij}(10)) \sum_{k=0}^{R-1} \binom{n-2}{k} \\ &\qquad + M_{ij}(11) \sum_{k=0}^{R-2} \binom{n-2}{k} \geq 2^{n-2} \end{aligned} \tag{13}$$

where the last term on the left is omitted if $R = 1$.

Furthermore,

$$M_{ij}(00) + M_{ij}(01) + M_{ij}(10) + M_{ij}(11) = |C| \quad (14)$$

$$M_{ij}(00) + M_{ij}(01) = M_i(0) \quad (15)$$

$$M_{ij}(00) + M_{ij}(10) = M_j(0). \quad (16)$$

Equation (12) (for $a = b = 0$) follows immediately from (13)–(16).

Another useful result on pairs of columns is the following.

Theorem 5: If C has length $n + 2$, covering radius $R + 1$, and fewer than $K(n, R)$ codewords, then $M_{ij}(ab) \geq 1$ for all i, j, a, b. In other words in any pair of coordinates there are codewords which assume all four possible values 00, 01, 10, and 11.

Proof: Suppose the first two coordinates are being considered, that is, $i = 1$, $j = 2$, and assume there is no codeword beginning with $00, \cdots$, that is, $M_{12}(00) = 0$. Let C_1 be the projection of C onto the first two coordinates, and C_2 the projection onto the last n coordinates. Since 00 is at distance ≥ 1 from C_1, $CR(C_1) \geq 1$. By hypothesis, $CR(C_2) \geq R + 1$. Therefore $CR(C) \geq CR(C_1) + CR(C_2) \geq R + 2$, a contradiction.

Corollary 6: The hypotheses of Theorem 5 imply that $M_i(a) \geq 2$ for all i and a, and

$$|C| \geq 4.$$

Proof: Immediate.

We now give two examples of lower bounds obtained by induction.

Theorem 7:

$$K(2R + 2, R) \geq 4$$

for $R = 1, 2, \cdots$.

Proof: This is true for $R = 1$ by (1), and then for all $R > 1$ by induction using Corollary 6.

Theorem 8:

$$K(2R + 3, R) \geq 7$$

for $R = 1, 2, \cdots$.

The case $R = 1$ was given in [28] and [30].

Proof: For $R = 1$ we must show $K(5, 1) \geq 7$. Suppose on the contrary that C is a $(5, 6)$ $R = 1$ code. By Theorem 3, $M_i(a) \geq 3$ for $a = 0$ and 1, and therefore $M_i(0) = M_i(1) = 3$, so the code is balanced. By Theorem 4,

$$M_{ij}(ab) \geq 1 \quad (17)$$

for all i, j, a, b. Without loss of generality the first codeword is 00000. Let us write the codewords in a $|C| \times n$ array, for example,

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \end{pmatrix}. \quad (18)$$

The columns are distinct, by (17). Ignore the first row. The five columns of length 5 each contain exactly two zeros and are therefore described by a subset of five edges from the complete graph on five vertices (the positions of the two zeros in a column specify an edge). It is easily verified that there are six ways to choose these five edges (one of which, corresponding to a five-cycle, is shown in (18)) and that none of these six codes has covering radius 1. (For example 11111 is at distance 2 from (18).) Thus $K(5, 1) \geq 7$.

For $R = 2$, suppose C is a $(7, 6)$ $R = 2$ code. From Corollary 6 we know $M_i(a) \geq 2$ for $a = 0, 1$. a) Suppose C contains at least two unbalanced coordinates. From Theorem 5 this implies (without loss of generality) that the array of codewords begins

$$\begin{pmatrix} 0 & 0 & \cdots \\ 0 & 1 & \cdots \\ 1 & 0 & \cdots \\ 1 & 1 & \cdots \\ 1 & 1 & \cdots \\ 1 & 1 & \cdots \end{pmatrix}. \quad (19)$$

But from Theorem 4, $M_{12}(00) \geq 2$, contradicting (19). b) If C contains a unique unbalanced column, then using Theorem 5 we can assume that the code is

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{pmatrix},$$

which can be completed in only one way, to

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

But this code has covering radius 3. c) If C is balanced, the first codeword can be taken as $\mathbf{0}$, and then the array is completed by choosing seven edges from the complete graph on five vertices. There are four ways to do this, and none of the codes has covering radius 2. Thus $K(7, 2) \geq 7$.

The case $R = 3$ is similar and is left to the reader. (Only one code needs to be tested.)

For $R \geq 4$ we can use induction, assuming the result is true for $R - 1$. Suppose C is a $(2R + 3, 6)$ R code. a) If there are ≥ 2 unbalanced coordinates, then by Theorem 5

we can assume that C begins

$$\begin{pmatrix} 0 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 0 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 1 & \cdot & \cdot & \cdots & \cdot & \cdot \\ 1 & 1 & \cdot & \cdot & \cdots & \cdot & \cdot \\ 1 & 1 & \cdot & \cdot & \cdots & \cdot & \cdot \end{pmatrix}.$$

But there are only eight possibilities for completing the last $n - 2 \geq 9$ columns. This forces a repeated column, contradicting Theorem 5. b) If there is a unique unbalanced column, then we have

$$\begin{pmatrix} 0 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \end{pmatrix}.$$

There are $\binom{4}{2} = 6$ possibilities for the last $n - 1 \geq 10$ columns, so there is a repeated column. c) If C is balanced, there are $\binom{5}{2} = 10$ possibilities for $n \geq 11$ columns, and again there is a repeated column. This completes the proof of Theorem 8.

C. Linear Inequalities

For a code $C \subseteq \mathbb{F}_2^n$, and an arbitrary vector $u \in \mathbb{F}_2^n$, let $A_i = A_i(u)$ denote the number of codewords at distance i from u, and let

$$a_i := \frac{1}{|C|} \sum_{u \in C} A_i(u). \tag{20}$$

Then

$$\sum_{i=0}^{n} A_i(u) = \sum_{i=0}^{n} a_i = |C| \tag{21}$$

$$A_i(u) \geq 0 \qquad a_i \geq 0 \qquad a_0 = 1. \tag{22}$$

The following inequalities were used by Stanton and Kalbfleisch [28]. If $CR(C) = 1$, then, since every vector must be within distance 1 of the code, we have

$$(n - i + 1)A_{i-1} + A_i + (i + 1)A_{i+1} \geq \binom{n}{i}, \tag{23}$$

for $i = 0, \cdots, n$ (with the convention that $A_j = 0$ for $j < 0$ or $j > n$). If $CR(C) = 2$, then

$$\binom{n - i + 2}{2} A_{i-2} + (n - i + 1)A_{i-1} + (1 + in - i^2)A_i + (i + 1)A_{i+1} + \binom{i + 2}{2} A_{i+2} \geq \binom{n}{i}, \tag{24}$$

for $i = 0, \cdots, n$. There are similar expressions for larger values of the covering radius.

By averaging over C, using (20), we see that the same inequalities hold for the a_i. For example, if $CR(C) = 1$, then

$$(n - i + 1)a_{i-1} + a_i + (i + 1)a_{i+1} \geq \binom{n}{i}. \tag{25}$$

The a_i must also satisfy the Delsarte inequalities [20, ch. 17]:

$$\sum_{i=0}^{n} a_i P_k(i) \geq 0, \tag{26}$$

for $k = 0, \cdots, n$, where $P_k(x)$ is a Krawtchouk polynomial.

The problem of finding a good covering code therefore leads to the following linear programming problem:

$$\text{minimize } a_0 + a_1 + \cdots + a_n$$

subject to (22), (25) or its generalization for larger R, and (26).

Theorem 9 (The Linear Programming Bound): If $s = a_0 + \cdots + a_n$ is the solution to this linear program, then $K(n, R) \geq s$.

Theorem 10:

a) $K(8,2) \geq 9$;

b) $K(9,2) \geq 13$;

c) $K(10,3) \geq 8$.

Proof: a) Suppose on the contrary that C is an $(8, 8)$ $R = 2$ code. Without loss of generality, we may assume $A_0 = 1$. Then (24) implies

$$\begin{aligned} 21A_1 + 6A_2 + 16A_3 + 4A_4 + 10A_5 &\geq 56 \\ 15A_2 + 5A_3 + 17A_4 + 5A_5 + 15A_6 &\geq 70 \\ 10A_3 + 4A_4 + 16A_5 + 6A_6 + 21A_7 &\geq 56 \\ 6A_4 + 3A_5 + 13A_6 + 7A_7 + 28A_8 &\geq 28 \\ 3A_5 + 2A_6 + 8A_7 + 8A_8 &\geq 8 \\ A_6 + A_7 + A_8 &\geq 1. \end{aligned} \tag{27}$$

To these we may add

$$\begin{aligned} A_1 + A_2 + \cdots + A_8 &= 7 \\ 0 \leq A_i &\leq 7 \ (1 \leq i \leq 7) \\ 0 \leq A_8 &\leq 1. \end{aligned} \tag{28}$$

It is easy to verify by computer that (27) and (28) have no integer solutions. b) Again there are no solutions. c) Suppose C is a $(10, 7)$ $R = 3$ code, and take $A_0 = 1$. The equations analogous to (23) and (24) read

$$\begin{aligned} 84A_1 + 28A_2 + 70A_3 + 25A_4 + 55A_5 + 15A_6 + 35A_7 &\geq 210 \\ 56A_2 + 21A_3 + 66A_4 + 26A_5 + 66A_6 + 21A_7 + 56A_8 &\geq 252 \\ 35A_3 + 15A_4 + 55A_5 + 25A_6 + 70A_7 + 28A_8 + 84A_9 &\geq 210 \\ 20A_4 + 10A_5 + 40A_6 + 22A_7 + 64A_8 + 36A_9 + 120A_{10} &\geq 120 \\ 10A_5 + 6A_6 + 24A_7 + 17A_8 + 45A_9 + 45A_{10} &\geq 45 \\ 4A_6 + 3A_7 + 10A_8 + 10A_9 + 10A_{10} &\geq 10 \\ A_7 + A_8 + A_9 + A_{10} &\geq 1, \end{aligned} \tag{29}$$

and we also have

$$A_1 + A_2 + \cdots + A_{10} = 6$$
$$0 \le A_i \le 6 \ (1 \le i \le 9)$$
$$0 \le A_{10} \le 1. \tag{30}$$

Equations (29) and (30) have four integral solutions, namely

i:	0	1	2	3	4	5	6	7	8	9	10
	1	0	0	0	2	3	0	0	1	0	0
	1	0	0	1	0	2	2	0	1	0	0
A_i:	1	0	0	1	1	1	2	1	0	0	0
	1	0	0	1	2	1	0	1	1	0	0

We must show that these are impossible. Let

$$n_4 := 84A_1 + 28A_2 + 70A_3 + 25A_4 + 55A_5 + 15A_6 + 35A_7,$$

so the first inequality in (29) reads $n_4 \ge 210$. For the first solution $n_4 = 215$, so only five vectors of weight 4 may be covered twice. Now two codewords of weight 5 and distance ≤ 6 apart cover at least 9 vectors of weight 4 twice. Therefore the three codewords of weight 5 must have mutual distances at least 8 apart, which is impossible. Similar arguments, of no greater difficulty, eliminate the other three cases.

Remark: Stanton and Kalbfleisch [28], [29] showed that $K(6,1) \ge 12$, $K(8,1) \ge 32$, $K(9,1) \ge 54$, and $K(10,1) \ge 96$. $K(9,1) \ge 54$ follows immediately from Theorem 1, and $K(10,1) \ge 96$ is weaker than the bound of 97 obtained from Theorem 1 (see Table I at the end of Section III).

III. Upper Bounds

A. Piecewise Constant Codes

We introduce a new family of codes, piecewise constant codes, defined as follows. The length n is partitioned as $n = n_1 + n_2 + \cdots + n_t$ (say), and each codeword c is partitioned in the same way, as

$$c = (c^{(1)}, c^{(2)}, \cdots, c^{(t)})$$

where length $(c^{(i)}) = n_i$. Then C is a *piecewise constant* code if it has the property that

if C contains one word with

$$wt(c^{(1)}) = w_1, \cdots, wt(c^{(t)}) = w_t,$$

then it contains all such words.

In other words the automorphism group of C contains all permutations in the first block of n_1 coordinates, all permutations in the second block of n_2 coordinates, and so on.

For example, Fig. 1 shows a piecewise constant code of length 5 corresponding to the partition $5 = 2 + 3$. There

00	000
00	111
10	000
01	000
11	011
11	101
11	110

Fig. 1. A (5,7) $R = 1$ piecewise constant code.

are seven codewords, corresponding to the weights

$$w_1 = 0, w_2 = 0, \quad 1 \text{ word},$$
$$w_1 = 0, w_2 = 3, \quad 1 \text{ word},$$
$$w_1 = 1, w_2 = 0, \quad 2 \text{ words},$$
$$w_1 = 2, w_2 = 2, \quad 3 \text{ words}. \tag{31}$$

Any piecewise constant code of length 5 partitioned as $5 = n_1 + n_2 = 2 + 3$ can be represented by a subset of the two-dimensional array of cells shown in Fig. 2. The cell at position (w_1, w_2) represents the set of vectors $c = (c^{(1)}, c^{(2)})$ with $wt(c^{(1)}) = w_1$, $wt(c^{(2)}) = w_2$. There are

$$\binom{n_1}{w_1}\binom{n_2}{w_2} = \binom{2}{w_1}\binom{3}{w_2}$$

such vectors, and this number is written in the cell. A piecewise constant code is then specified by circling some of the cells in the array, and the number of codewords is the sum of the circled numbers. The four circled cells in Fig. 2 represent the code of Fig. 1, and there are a total of seven codewords.

w_1 \ w_2	0	1	2	3
0	(1)	3	3	(1)
1	(2)	6	6	2
2	1	3	(3)	1

Fig. 2. Two-dimensional array representing the code of Fig. 1.

Piecewise constant codes have the desirable property that the covering radius R is easy to calculate from this array of cells. This is because R is simply the maximal distance of any cell from the code (i.e., from the nearest circled cell), when the distance between two cells is measured in the Manhattan metric. In Fig. 2 the Manhattan distance between two cells is the number of horizontal and vertical steps needed to move from one to the other.

In general a piecewise constant code corresponding to a partition $n = n_1 + \cdots + n_t$ is described by a t-dimensional array of cells, and the Manhattan distance between two cells $(w_1, \cdots, w_t)$ and $(w_1', \cdots, w_t')$ is $|w_1 - w_1'| + \cdots + |w_t - w_t'|$. In Fig. 2 it is clear that every cell is within Manhattan distance 1 of a circled cell, so the covering radius is 1. Thus $K(5,1) \le 7$, and in view of

Theorem 8 this is optimal: $K(5,1) = 7$. This code was first found in 1948, using a different method, by Taussky and Todd [30] and was shown to be unique by Stanton and Kalbfleisch [28].

000	100
000	010
000	001
100	111
010	111
001	111
011	000
101	000
110	000
111	011
111	101
111	110

Fig. 3. A $(6,12)$ $R = 1$ piecewise constant code.

A second example of a piecewise constant code is given in Figs. 3 and 4. This corresponds to the partition $6 = 3 + 3$ and contains 12 codewords. Fig. 4 shows the "spheres" of Manhattan radius 1 around the codewords, proving that $R = 1$. Thus $K(6,1) = 12$. A code with 12 codewords and $R = 1$ was found by Stanton and Kalbfleisch in [28], but there is an error in the published version of their code (it has $R = 2$), so we cannot tell if the codes are equivalent.

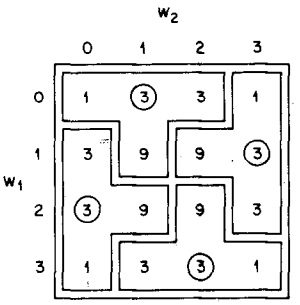

Fig. 4. Two-dimensional array representing the code of Fig. 3 and showing the Manhattan "spheres" of radius 1 around the marked cells.

Piecewise constant codes partitioned into $t \leq 4$ parts can be constructed by hand. It makes an amusing puzzle to try and place pennies on the cells so as to minimize the sum of the numbers under the pennies while ensuring that every cell is within Manhattan distance R of some penny. The reader may like to try finding an $(8,15)$ $R = 2$ code, based on the partition $8 = 4 + 4$. (Since we shall construct a better code in the following section, we omit the solution.)

We now give two further examples. Fig. 5 shows a piecewise constant $(2R + 3, 7)R$ code, based on the partition $n = (2R - 1) + 3 + 1$ into three parts. The figure shows certain key boundaries of the Manhattan spheres of radius R, enough to show that all the points are covered.

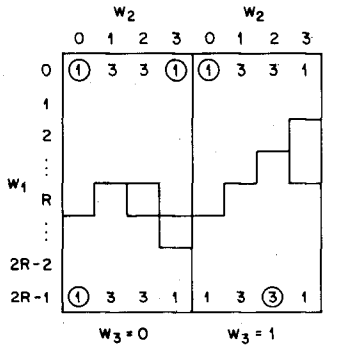

Fig. 5. Three-dimensional array showing a piecewise constant code proving that $K(2R + 3, R) \leq 7$. Interior lines show some key boundaries of the Manhattan spheres of radius R.

In view of Theorem 8, this proves that

$$K(2R + 3, R) = 7 \tag{32}$$

for $R = 1, 2, \cdots$.

Fig. 6 shows a code that establishes

$$K(2R + 4, R) \leq 12, \tag{33}$$

based on the partition $n = (2R - 2) + 3 + 3$. Again we show the most important boundaries of the spheres around the codewords.

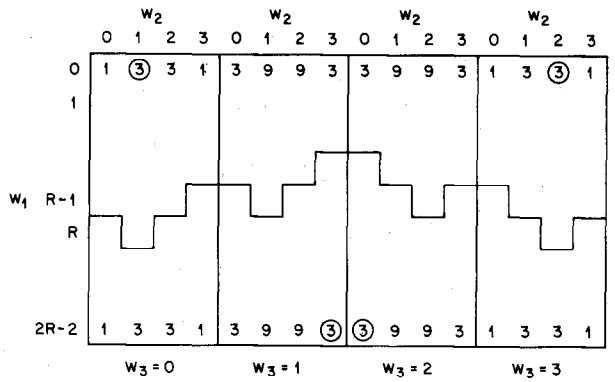

Fig. 6. Piecewise constant code proving that $K(2R + 4, R) \leq 12$.

Our final example in this section is an $(11, 192)$ $R = 1$ code, obtained by combining a piecewise constant code and a Steiner system. The codewords are written $c = (c^{(1)}, c^{(2)})$, where length $(c^{(1)}) = 6$ and length $(c^{(2)}) = 5$, and consist of the following:

all 5 words with $wt(c^{(1)}) = 0$, $wt(c^{(2)}) = 1$
all 10 words with $wt(c^{(1)}) = 0$, $wt(c^{(2)}) = 2$
all 15 words with $wt(c^{(1)}) = 2$, $wt(c^{(2)}) = 0$
the 66 blocks of the Steiner system $S(4,5,11)$
and the complements of all the above words. (34)

The vectors of weight ≤ 3 and ≥ 8 are covered by the piecewise constant part of the code, as shown in Fig. 7. Vectors of weight 4 are covered by the Steiner system. Vectors of weight 5 are either in the Steiner system or are

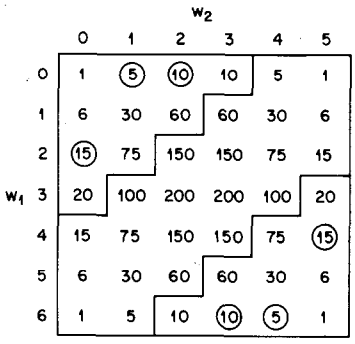

Fig. 7. Shows how vectors of weight ≤ 3 and ≥ 8 are covered by the code of (34).

covered by one of the complementary blocks (since the blocks and their complements together form the Steiner system $S(5,6,12)$ with one coordinate deleted). Thus

$$K(11,1) \leq 192. \tag{35}$$

B. Normal Codes and the ADS Construction

The concept of a normal *linear* code was introduced in [10] and is easily extended to nonlinear codes. Let C be an arbitrary binary code of length n and covering radius R. For $i = 1, \cdots, n$, $a = 0,1$ let $C_a^{(i)}$ denote the subset of codewords $(c_1, \cdots, c_n)$ with $c_i = a$, and for an arbitrary vector $x \in \mathbb{F}_2^n$ let

$$f_a^{(i)}(x) := d\left(x, C_a^{(i)}\right)$$

(with the convention that $f_a^{(i)}(x) = n$ if $C_a^{(i)}$ is empty). Then

$$N^{(i)} := \max_x \left\{ f_0^{(i)}(x) + f_1^{(i)}(x) \right\} \tag{36}$$

is called the *norm of C with respect to the ith coordinate*. If

$$N^{(i)} \leq N \tag{37}$$

for at least one coordinate i, we say that C has *norm* N, and coordinates i for which (37) holds are called *acceptable*. Finally, a code is *normal* if it has norm N satisfying

$$N \leq 2R + 1. \tag{38}$$

Remark: In order for Theorem 11 to hold, we deliberately do not[1] insist that equality holds in (37) for some i. This means that if a code has norm N, it also has norm $N+1, N+2, \cdots$. Of course we always choose N as small as possible.

The following properties now follow exactly as in [10]. A code of norm N has covering radius

$$R \leq \left\lfloor \frac{N}{2} \right\rfloor. \tag{39}$$

A code is normal if and only if we can take

$$N = 2R \text{ or } 2R + 1. \tag{40}$$

[1] This definition of norm differs slightly from that given in [10]. The present definition is preferable, for otherwise in the ADS construction it is not clear that the overlapping coordinate is always acceptable (cf. Theorem 11).

If the weight of every codeword is even, N can be taken to be even (but not conversely).

Many examples of normal linear codes are given in [10], and further examples will be found in Section IV. It is easily verified by computer that the $(5,7)1$, $(6,12)1$, and $(11,192)1$ nonlinear codes constructed in the previous section are normal, and all coordinates are acceptable.

Normal codes may be combined efficiently using the amalgamated direct sum construction, introduced in [10] for linear codes. Let A be an (n_A, M_A) R_A normal code in which the last coordinate is acceptable and $A_0^{(n_A)}$, $A_1^{(n_A)}$ are nonempty, and let B be an (n_B, M_B) R_B normal code in which the first coordinate is acceptable and $B_0^{(1)}$, $B_1^{(1)}$ are nonempty. Then their amalgamated direct sum (ADS)

$$A \oplus B$$

is the code of length $n_A + n_B - 1$ consisting of the codewords

$$(a,0,b) \text{ and } (c,1,d) \tag{41}$$

where $(a,0) \in A_0^{(n_A)}, (0,b) \in B_0^{(1)}, (c,1) \in A_1^{(n_A)}, (1,d) \in B_1^{(1)}$.

Theorem 11: The amalgamated direct sum $A \oplus B$ contains

$$|A_0^{(n_A)}||B_0^{(1)}| + |A_1^{(n_A)}|B_1^{(1)}| \tag{42}$$

codewords,

$$\text{norm}(A \oplus B) = \text{norm}(A) + \text{norm}(B) - 1 \tag{43}$$

and the n_Ath coordinate is acceptable, and

$$CR(A \oplus B) \leq R_A + R_B. \tag{44}$$

If the covering radius of $A \oplus B$ is $R_A + R_B$, then $A \oplus B$ is normal.

Proof: Let $C = A \oplus B$, of length $n := n_A + n_B - 1$ and covering radius R_C. Equation (42) follows immediately from (41). For a vector $z = (x,0,y) \in \mathbb{F}_2^n$, the function $f_0^{n_A}(z)$ (for C) can be expressed in terms of $f_0^A := f_0^{n_A}$ (for A) and $f_0^B := f_0^1$ (for B) as

$$f_0^{n_A}(z) = f_0^A(x,0) + f_0^B(0,y),$$

and, similarly,

$$f_1^{n_A}(z) = f_1^A(x,0) + f_1^B(0,y) - 1.$$

Therefore

$$f_0^{n_A}(z) + f_1^{n_A}(z) \leq \text{norm}(A) + \text{norm}(B) - 1.$$

The same conclusion holds if $z = (x,1,y)$. Therefore (43) is true. From (39) and (40) we have

$$\begin{aligned} 2R_C &\leq \text{norm}(C) \\ &= \text{norm}(A) + \text{norm}(B) - 1 \\ &\leq 2R_A + 2R_B + 1, \end{aligned} \tag{45}$$

so $R_C \leq R_A + R_B$. Finally, if $R_C = R_A + R_B$, $\text{norm}(C) \leq 2R_C + 1$ follows from (45).

Examples of Amalgamated Direct Sums:

1)

$$(5,7)1 \dot{\oplus} (3,2)1 = (7,7)2$$
$$(7,7)2 \dot{\oplus} (3,2)1 = (9,7)3$$
$$(9,7)3 \dot{\oplus} (3,2)1 = (11,7)4$$

and so on. These are piecewise constant codes, and are shown in Fig. 5.

2)

$$(6,12)1 \dot{\oplus} (3,2)1 = (8,12)2$$
$$(8,12)2 \dot{\oplus} (3,2)1 = (10,12)3$$

and so on. This is a different sequence of $(2R + 4, 12)R$ piecewise constant codes from that shown in Fig. 6.

3)

$$(5,7)1 \dot{\oplus} (7,16)1 = (11,56)2$$
$$(11,56)2 \dot{\oplus} (3,2)1 = (13,56)3$$

and so on.

4)

$$(6,12)1 \dot{\oplus} (7,16) = (12,96)2.$$

C. The Partitioning Property

The construction described here sometimes provides an alternative to the ADS construction, but requires that the initial code satisfies a seemingly stronger condition than normality. An $(n, M)R$ code C is said to have the *partitioning property* if there is a partition of C into two nonempty subsets C' and C'' such that

$$\begin{aligned} &\text{for } x \in \mathbb{F}_2^n \setminus C', d(x, C'') \le R + 1 \\ &\text{for } x \in C', \quad d(x, C'') \le R + 2 \\ &\text{for } x \in \mathbb{F}_2^n \setminus C'', d(x, C') \le R + 1 \\ &\text{for } x \in C'', \quad d(x, C') \le R + 2. \end{aligned} \tag{46}$$

For example, the (5, 7)1 code of Fig. 1 has the partitioning property since we may take $C' = \{00000, 00111, 01000\}$, $C'' = \{10000, 11011, 11101, 11110\}$. The (6, 12)1 code of Fig. 3 also has the partitioning property. But the normal code $\{0^n, 1^n\}$ does not, for $n \ge 5$.

Theorem 12: If C is an $(n, M)R$ code with the partitioning property, and $R \ge 1$, then there is an $(n + 2p, M)R + p$ code C^* for $p = 0, 1, 2, \cdots$.

Proof: Let C^* consist of the codewords $(c', 0^{2p})$ and $(c'', 1^{2p})$ for $c' \in C', c'' \in C''$. Consider an arbitrary $w = |x|y| \in \mathbb{F}_2^{n+2p}$, and let $k = wt(y)$. By symmetry we may assume $0 \le k \le p$. If $k = p$, a vector $u \in C'$ exists with $d(u, x) \le R$ and $d(|u|0^{2p}|, w) \le R + p$. If $k = p - 1$ and $x \in C''$, then $d(|x|1^{2p}|, w) = p + 1 \le R + p$. If $k = p - 1$ and $x \notin C''$, then there is $c' \in C'$ with $d(c', x) \le R + 1$ and $d(|c'|0^{2p}|, w) \le R + p$. Finally, if $k \le p - 2$, there is $c' \in C'$ with $d(x, c') \le R + 2$, and $d(|c'|0^{2p}|, w) \le R + p$.

Theorem 12 gives an alternative way of obtaining $K(2R + 3, R) \le 7$ and (33).

D. A Variation on the $|u|u + v|$ Construction

Mollard [23] and, independently, Katsman and Litsyn [15] have found a construction for codes of covering radius 1 that is a variation on the $|u|u + v|$ construction described in [20] and [25].

Theorem 13 (Mollard [23], Katsman and Litsyn [15]): Let C be an (n, M) $R = 1$ code. Then the code C^* consisting of the codewords

$$|u|u + v|\pi(u)| \tag{47}$$

for $u \in \mathbb{F}_2^n$, $v \in C$ and

$$\pi(u) = \begin{cases} 0 & \text{if } wt(u) \text{ is even,} \\ 1 & \text{if } wt(u) \text{ is odd,} \end{cases}$$

is a $(2n + 1, 2^n M)$ $R = 1$ code.

Proof: Consider an arbitrary $w = |x|y|z| \in \mathbb{F}_2^{2n+1}$. There is a codeword $v \in C$ such that $d(x + y, v) \le 1$. If either $d(x + y, v) = 0$ or $\pi(x) = z$, then

$$c = |x|x + v|\pi(x)|$$

satisfies $d(c, w) \le 1$. Otherwise, change x in one coordinate to obtain a vector x^* such that $x^* + y = v \in C$, and then $\pi(x^*) = z$ and

$$c^* = |x^*|x^* + v|\pi(x^*)|$$

satisfies $d(c^*, w) = 1$.

For example, if $C = (11, 192)1$, then $C^* = (23, 3 \cdot 2^{17})1$.

E. Special Cases

The following theorem assembles what is known about $K(n, R)$ for $n \le 2R + 4$.

Theorem 14: For all $R \ge 1$,

$$K(1, R) = K(2, R) = \cdots = K(R, R) = 1 \tag{48}$$

$$\begin{aligned} K(R + 1, R) &= K(R + 2, R) \\ &= \cdots = K(2R + 1, R) = 2 \end{aligned} \tag{49}$$

$$K(2R + 2, R) = 4 \tag{50}$$

$$K(2R + 3, R) = 7 \tag{51}$$

$$7 \le K(2R + 4, R) \le 12. \tag{52}$$

Proof: Equations (48) and (49) are immediate. Equation (50) is obtained from Theorem 7 and linear codes. For (51) see (32). Finally (52) follows from (33) and

$$K(n + 1, R) \ge K(n, R). \tag{53}$$

Table I gives the known bounds on $K(n, R)$ for $n \le 23$ and $R \le 4$.

Key to Table I: This key indicates the *simplest* proof of a given result, not necessarily the *earliest*. Unmarked lower bounds are from the sphere bound (1). Unmarked upper

TABLE I[a]
BOUNDS ON $K(n, R)$ THE MINIMAL NUMBER OF CODEWORDS IN ANY BINARY CODE OF LENGTH n AND COVERING RADIUS R

n	$R=1$	$R=2$	$R=3$	$R=4$
1	1	1	1	1
2	2	1	1	1
3	2	2	1	1
4	4	2	2	1
5	$^{a}7^{p}$	2	2	2
6	$^{x}12^{p}$	$^{a}4$	2	2
7	16	$^{a}7^{q}$	2	2
8	$^{x}32$	$^{d}9$–12^{q}	$^{a}4$	2
9	$^{b}54$–64	$^{d}13$–16	$^{a}7^{q}$	2
10	$^{b}97$–128	$^{b}20$–32	$^{d}8$–12^{q}	$^{a}4$
11	$^{b}174$–192^{p}	$^{b}32$–56^{q}	$^{b}10$–16	$^{a}7^{q}$
12	$^{b}326$–384^{r}	$^{b}54$–96^{q}	$^{c}15$–32	$^{e}7$–12^{q}
13	$^{b}598$–768^{r}	$^{b}91$–128	$^{b}23$–56^{q}	$^{c}9$–16
14	$^{b}1103$–1536^{r}	$^{b}157$–256	$^{b}36$–64	$^{b}12$–32
15	2048	$^{b}272$–512	$^{b}58$–128	$^{b}18$–56^{q}
16	$^{b}3933$–4096	$^{b}485$–1024	$^{c}97$–256	$^{b}27$–64
17	$^{b}7373$–2^{13}	$^{b}859$–2^{11}	$^{b}160$–512	$^{b}42$–128
18	$^{b}13879$–2^{14}	$^{b}1533$–2^{12}	$^{b}268$–2^{10}	$^{b}66$–256
19	$^{b}26216$–2^{15}	$^{b}2758$–2^{12}	$^{b}456$–2^{10}	$^{b}106$–512
20	-2^{16}	$^{b}4996$–2^{13}	$^{b}781$–2^{11}	$^{b}171$–512
21	-2^{17}	$^{b}9096$–2^{14}	$^{b}1347$–2^{12}	$^{c}281$–2^{10}
22	-2^{18}	$^{b}16580$–2^{15}	$^{b}2342$–2^{12}	$^{c}464$–2^{11}
23	$-3\cdot 2^{17\,s}$	$^{b}30421$–2^{16}	4096	$^{c}774$–2^{12}

[a] See text for key.

bounds are linear codes from [10]:

- *a* Theorems 7 and 8,
- *b* Theorem 1,
- *c* Theorem 2,
- *d* Theorem 10,
- *e* from (53),
- *p* piecewise constant code (Section III-A),
- *q* amalgamated direct sum (Section III-B),
- *r* by taking $C \oplus \{0,1\}$ we always have

$$K(n+1, R) \le 2K(n, R), \tag{54}$$

- *s* Theorem 13,
- *x* Stanton and Kalbfleisch [28], [29].

IV. Normal Linear Codes

At the present time it is not known if an abnormal linear code exists. In this section we give some results, stronger than those in [10], which imply that certain linear codes are normal. Throughout this section C denotes an $[n, k, d]$ linear code of covering radius R. The following theorem assembles some results from [10].

Theorem 15: a) If C is normal, then so is any code obtained by appending any number of zeros to the codewords of C.

b) If C is normal, then so is the code obtained by adding an overall parity check to C.

c) If C has no coordinate which is identically zero, then

$$\text{norm}(C) \le \text{length}(C).$$

d) A perfect code is normal.

e) A direct sum of normal codes is normal.

f) If $\dim(C) \le 2$, then C is normal.

g) If length $(C) \le 8$, then C is normal.

Our main goal in this section is to prove Theorem 32, which considerably strengthens f) and g).

In view of Theorem 15a), we may always assume (when proving that classes of codes are normal) that C has no coordinate which is identically zero. This implies $R \le [n/2]$.

It is convenient to have a name for vectors for which $f_0^{(i)}(x) + f_1^{(i)}(x)$ is large (see (36)). A vector x is called *bad for coordinate i* if

$$f_0^{(i)}(x) + f_1^{(i)}(x) \ge 2R + 2. \tag{55}$$

Then C is abnormal if and only if for all i there is a vector x (depending on i) that is bad for i. The first lemma asserts that bad vectors must be "mismatched" with $C_0^{(i)}$ and $C_1^{(i)}$.

Lemma 16: Suppose $x = (x_1 \cdots x_n)$ is bad for coordinate i and satisfies $d(x, C) = R$. If $d(x, C_0^{(i)}) = R$, then $x_i = 1$, while if $d(x, C_1^{(i)}) = R$, then $x_i = 0$.

Proof: Otherwise complementing x_i leads to a vector further than R from the code.

The next lemma gives a simple sufficient condition for normality. Note that since C is linear, $CR(C_0^{(i)}) = CR(C_1^{(i)})$.

Lemma 17: If C has covering radius R, and if, for some i, either

$$CR\left(C_0^{(i)}\right) \le R + 2$$

or

$$CR\left(C_1^{(i)}\right) \le R + 2,$$

then C is normal.

Proof: Assume $CR(C_1^{(i)}) \le R + 2$, and suppose x is bad for i. Then either $f_0^{(i)}(x) \le R$ or $f_1^{(i)}(x) \le R$. Now $f_0^{(i)}(x + c) = f_0^{(i)}(x)$ if $c \in C_0^{(i)}$, while $f_0^{(i)}(x + c) = f_1^{(i)}(x)$ if $c \in C_1^{(i)}$. So we may assume $f_0^{(i)}(x) \le R$. From (55), $f_1^{(i)}(x) \ge R + 2$. Therefore, by hypothesis, $f_1^{(i)}(x) = R + 2$ and $f_0^{(i)}(x) = R$. From Lemma 16, $x_i = 1$. Let y be obtained by complementing the ith coordinate of x. Then $f_0^{(i)}(y) = R - 1$, $f_1^{(i)}(y) = R + 3$, which contradicts the hypothesis. Therefore no vector is bad for i, so $\text{norm}(C) \le 2R + 1$ and C is normal.

Let C have minimal distance d. Coordinate i is said to be *good* if

$$d\left(C_0^{(i)}, C_1^{(i)}\right) = d. \tag{56}$$

A coordinate is good if and only if it is in the support of a vector of minimal weight (so good coordinates always exist). By linearity, if i is good, then for all $c_1 \in C_1^{(i)}$ there is $c_0 \in C_0^{(i)}$ with $d(c_0, c_1) = d$.

Lemma 18: If coordinate i is good, then

$$CR\left(C_0^{(i)}\right) \le R + d \text{ and } CR\left(C_1^{(i)}\right) \le R + d. \tag{57}$$

Proof: For any x, $d(x, C) \le R$, and the triangle inequality implies (57).

Theorem 19: If $d \le 2$, C is normal and all good coordinates are acceptable.

Proof: Lemmas 17 and 18.

Theorem 20: If $R \le 1$, C is normal.

Proof: The result is immediate if $R = 0$, so assume $R = 1$, Since

$$d \le 2R + 1 \tag{58}$$

[10, eq. (13)], $d \le 3$. If $R = 1$ and $d = 3$, C is perfect, hence normal. Otherwise $d \le 2$, and C is normal by Theorem 19.

Lemmas 21 and 23 assert that if x is bad for i, not only is $f_0^{(i)}(x) + f_1^{(i)}(x)$ large, but the individual quantities $f_0^{(i)}(x)$ and $f_1^{(i)}(x)$ cannot be too small.

Lemma 21: If C is abnormal, then for all good i, and all x bad for i,

$$d(x, C) \ge 2.$$

Proof: Suppose $i = 1$ is good, and x is bad for i. Write $C_0 := C_0^{(i)}$, $C_1 := C_1^{(i)}$. 1) If $x \in C$, say $x \in C_1$, then $f_0^{(i)}(x) \ge 2R + 2$. But since i is good, $f_0^{(i)}(x) = d \le 2R + 1$ by (58), a contradiction. 2) Suppose $d(x, C) = 1$, say $f_1^{(i)}(x) = 1$, and $d(x, c_1) = 1$ for some $c_1 \in C_1$. Therefore $f_0^{(i)}(x) \ge 2R + 1$, and $d = d(c_1, C_0) \ge 2R$ by the triangle inequality. If $d \ge 2R + 1$, then C is perfect, hence normal. Thus $d = 2R$ and $f_0^{(i)}(x) = 2R + 1$.

If $x = 0x'$, then $y = 1x'$ satisfies $y \in C_1$, $d = d(y, C_0) = 2R + 2$, contradicting (58). If $x = 1x'$, then $y = 0x'$ satisfies $f_0^{(i)}(y) = 2R$, $f_1^{(i)}(y) = 2$, and for all $c_1' \in C_1$, $c_1' \ne c_1$, we have $d(c_1, c_1') \ge d$, $d(c_1', x) \ge d - 1 = 2R - 1$, $d(c_1', y) > d(c_1', x)$, so $d(c_1', y) \ge 2R$. Then we can find a vector z such that $d(z, y) = R - 1$ and $d(z, c_1) = R + 1$. Therefore $d(z, c_1') \ge 2R - (R - 1) = R + 1$, and similarly $d(z, C_0) \ge d(y, C_0) - d(y, z) \ge R + 1$. Thus $d(z, C) \ge R + 1$, a contradiction.

Theorem 22: If $R \le 2$, C is normal.

Proof: By Theorem 20 we may assume $R = 2$. Suppose C is abnormal. Then there is a good coordinate i and an x bad for i. By Lemma 21, $d(x, C) = 2$, say $f_1^{(i)}(x) = 2$, $f_0^{(i)}(x) \ge 2R = 4$. By Lemma 16, $x_i = 0$. If y is obtained by complementing the ith coordinate of x, $f_0^{(i)}(y) = 5$, $f_1^{(i)}(y) = 1$, and y is bad for i, contradicting Lemma 21.

Theorem 22 establishes the normality of the $[59, 49]$ $R = 2$ code given in [10, fig. 4].

Lemma 23: If x is bad for some good coordinate i, then

$$d(x, C) \ge R + 1 - d/2. \tag{59}$$

Proof: Without loss of generality $d(x, C) = f_1^{(i)}(x) \le f_0^{(i)}(x)$. From (55), $f_0^{(i)}(x) \ge 2R + 2 - f_1^{(i)}(x)$. Since i is good, $f_0^{(i)}(x) \le f_1^{(i)}(x) + d$. Therefore $2f_1^{(i)}(x) = 2d(x, C) \ge 2R + 2 - d$.

Theorem 24: If $d \le 3$, C is normal.

Proof: Suppose C is abnormal. Let i be good, and let x be bad for i. From Theorem 19, $d = 3$. From Lemma 23, $d(x, C) = R$, say $f_1^{(i)}(x) = R$, $f_0^{(i)}(x) \ge R + 2$. By Lemma 16, $x_i = 0$. Then complementing the ith coordinate contradicts Lemma 23.

The proof shows that if $d = 3$, then every coordinate in the support of a codeword of weight 3 is acceptable.

To obtain further results, we distinguish between two cases:

I: every coordinate of C is repeated at least once, or
II: C contains a unique coordinate.

Stated another way, in case I every column in a generator matrix for C occurs at least twice, while in case II there is at least one unique column.

Suppose C contains n_1 columns of one type, n_2 columns of a second type, $\cdots$. Then $S(C) := \langle n_1, n_2, \cdots, n_p \rangle$ is called the *signature* of C (cf. [5]). Case I obtains if and only if all $n_i \ge 2$. If R is small compared with n, then case II obtains.

Lemma 25: If $R < n/3$, then C contains a unique column.

Proof: Suppose the contrary, so that all $n_i \ge 2$. Write $n_i = 2m_i + \epsilon_i$, $\epsilon_i = 0$ or 1. By permuting the coordinates, we obtain a generator matrix for C of the form $[AB]$, where there are $n^{(A)} = 2\sum m_i$ columns in A, each column occurring an even number of times, and $n^{(B)} = \sum \epsilon_i$ columns in B. Then $n^{(A)} \ge 2n^{(B)}$, so $n^{(A)} \ge 2n/3$, and (cf. [5, sec. II-D]) $CR(A) \ge n^{(A)}/2$, so $R \ge n/3$.

$\tilde{C}$, the *contraction* of C, is obtained by taking just one column of each type. The length of $\tilde{C}$ will be denoted by p.

Lemma 26:

$$\dim \tilde{C} := \dim C = k \tag{60}$$

$$p := \text{length}\,(\tilde{C}) \ge k \tag{61}$$

$$\min n_i \le d, \text{with equality if } p = k \tag{62}$$

where d is the minimal distance of C.

The elementary proof is omitted. We first deal with case I.

Theorem 27: If every coordinate of C is repeated, and length $(C) \le 12$, then C is normal.

Proof: Let C be an $[n, k, d]$ code of covering radius R and norm N. From Theorem 15 we may assume $k \ge 3$.

a) $k = 3$. Then $p \ge 3$ by (61).

a1) $p = 3$. Then $n_i \ge d$ by (62), $d \ge 4$ by Theorem 24, so $n \ge 12$. If $n = 12$, then $S(C) = \langle 4, 4, 4 \rangle$, and $\tilde{C}$ has length 3 and dimension 3. Since $\tilde{C}$ is decomposable, so is C, and therefore C is normal by Theorem 15e).

a2) $p = 4$. If $n = 8$, C is normal by Theorem 15g). If $n = 9$, then $S(C) = \langle 3, 2, 2, 2 \rangle$, $R \ge 4$ (by inspection), $N \le 9$ (by Theorem 15c)), and C is normal. If $n = 10$, $S(C)$ is either $\langle 4, 2, 2, 2 \rangle$, $R = 5$, normal, or $\langle 3, 3, 2, 2 \rangle$, which requires further study and is dealt with later. If $n = 11$, then $S(C)$ is $\langle 5, 2, 2, 2 \rangle$, $\langle 4, 3, 2, 2 \rangle$, or $\langle 3, 3, 3, 2 \rangle$. The first two have $R = 5$ and are normal, and the latter is

dealt with below. If $n = 12$, there are three difficult cases, $\langle 5,3,2,2\rangle$, $\langle 4,3,3,2\rangle$, and $\langle 3,3,3,3\rangle$.

a3) $p = 5$. There is only one difficult case, when $n = 12$ and $S(C) = \langle 3,3,2,2,2\rangle$.

b) $k = 4$.

b1) $p = 4$ implies $n_i \geq 4$ and $n \geq 16$.

b2) For $p = 5$ there is one difficult case, $\langle 3,3,2,2,2\rangle$.

c) The cases with $k \geq 5$ are easily disposed of.

It remains to show that the following codes are normal: any code of dimension 3 and signature $\langle 3,3,2,2\rangle$, $\langle 3,3,3,2\rangle$, $\langle 5,3,2,2\rangle$, $\langle 4,3,3,2\rangle$, $\langle 3,3,3,3\rangle$ or $\langle 3,3,2,2,2\rangle$; or any code of dimension 4 and signature $\langle 3,3,2,2,2\rangle$. We give the details of the last case only, the others being similar. $\tilde{C}$ is a $[5,4]$ code with minimal distance $\tilde{d} \geq 2$ (otherwise, $\tilde{C}$ is decomposable) and is therefore unique; $\tilde{C}$ is the even weight code of length 5. Then C is unique and has generator matrix

$$\begin{bmatrix} 1&1&1&0&0&0&0&0&0&0&1&1\\ 0&0&0&1&1&1&0&0&0&0&1&1\\ 0&0&0&0&0&0&1&1&0&0&1&1\\ 0&0&0&0&0&0&0&0&1&1&1&1 \end{bmatrix}.$$

This code is easily checked by computer to have covering radius 5 and to be normal. This completes the proof of Theorem 27.

We next consider case II. For the rest of this section we assume that C has length $n \geq 2$, has no coordinate which is identically zero, and contains a unique coordinate, which we take to be the first coordinate.

Lemma 28: If $x = 0x'$, then

$$f_0^{(1)}(x) \leq \frac{n-1}{2} \qquad f_1^{(1)}(x) \leq \frac{n+1}{2}, \tag{63}$$

while if $x = 1x'$,

$$f_0^{(1)}(x) \leq \frac{n+1}{2} \qquad f_1^{(1)}(x) \leq \frac{n-1}{2}. \tag{64}$$

In either case

$$f_0^{(1)}(x) + f_1^{(1)}(x) \leq R + \frac{n+1}{2}. \tag{65}$$

Proof: The hypotheses imply that in coordinates 1 and j $(2 \leq j \leq n)$, each of 00, 01, 10, and 11 occurs equally often. Let C_a' be obtained by deleting the first coordinate of $C_a^{(1)}$ ($a = 0$ or 1). Then, for any $x' \in \mathbb{F}_2^{n-1}$,

$$2^{-(k-1)} \sum_{c' \in C_a'} d(x', c') = \frac{1}{2}(n-1),$$

which proves (63) and (64). Equation (65) follows because $\min\{f_0^{(1)}(x), f_1^{(1)}(x)\} \leq R$.

Corollary 29: If, for some x,

$$f_0^{(1)}(x) + f_1^{(1)}(x) = n,$$

then n is odd.

Proof: This follows immediately from (63) and (64).

Equation (65) can be strengthened slightly.

Lemma 30: Suppose the first coordinate of C is unique, and assume x is bad for the first coordinate. Then

$$f_0^{(1)}(x) + f_1^{(1)}(x) \leq R + \frac{n-1}{2}. \tag{66}$$

Proof: From (65) we must show that a) $f_0^{(1)}(x) + f_1^{(1)}(x) \neq R + (n+1)/2$ when n is odd, and b) $f_0^{(1)}(x) + f_1^{(1)}(x) \neq R + n/2$ when n is even. a) Suppose $x = 0x'$. Then $f_0^{(1)}(x) + f_1^{(1)}(x) = R + (n+1)/2$ implies, from (63), $f_0^{(1)}(x) = R$, $f_1^{(1)}(x) = (n+1)/2$. But this contradicts Lemma 16. A similar argument applies in case b).

Theorem 31: If C contains a unique coordinate and is abnormal, then

$$n \geq 2R + 5. \tag{67}$$

In particular, $n \geq 11$.

Proof: Equation (67) follows from (55) and (66). The second assertion then follows from Theorem 22.

A computer search was used to show that all codes of length 11 and 12 are normal. In view of the preceding results (in particular Theorems 15, 19, and 22), and the known bounds on minimal distance [11] and covering radius [10], this required the study of all codes with $n = 11$, $k = 4$, 5, or 6, $d = 4$ or 5, and $R = 3$; or $n = 12$, $k = 5$, 6, or 7, $d = 4$, and $R = 3$. Using the Bell Laboratories Cray-1 computer, all such codes were shown to be normal.

Collecting the above results, we have the following theorem.

Theorem 32: If C has length $n \leq 12$, or dimension $k \leq 2$, or minimal distance $d \leq 3$, or covering radius $R \leq 2$, then C is normal.

V. Some Conjectures

As in [5] and [10] let $k[n, R]$ be the smallest k for which an $[n, k]R$ code exists, let $t[n, k]$ be the smallest R for which an $[n, k]R$ code exists, and let $t(n, K)$ be the smallest R for which an $(n, K)R$ code exists. In this section we state some conjectures concerning these functions and $K(n, R)$ (defined in Section II).

Conjectures

A: For $k > 1$,

$$t[n+2, k] \leq t[n, k] + 1 \text{ and}$$
$$t(n+2, k) \leq t(n, k) + 1, \qquad k > 1.$$

B: For $R \neq n$,

$$k[n+2, R+1] \leq k[n, R].$$

C: For $R \neq n$,

$$K(n+2, R+1) \leq K(n, R).$$

It is shown in [16] that conjecture C is equivalent to the nonlinear version of conjecture A. The following conjecture is stronger.

Conjecture

D: Among the optimal covering codes (i.e., those attaining $t[n, k]$, $k[n, R]$ or $K(n, R)$) it is always possible to find a normal code.

For in view of the ADS construction (compare Theorem 11 and [10, theorem 20]), conjecture D implies A, B, and C. We have already mentioned the conjecture that among the optimal covering codes it is always possible to find a balanced code.

Conjecture B was shown to be true for fixed R and all sufficiently large n in [5]. We now prove a similar result for conjecture C.

Theorem 33: For fixed R there is an N_0 such that, for $n \geq N_0$,

$$K(n+2, R+1) \leq K(n, R). \tag{68}$$

Proof: By using shortened Hamming codes, we have

$$k[n,1] = n - [\log_2 (n+1)];$$

and by taking direct sums

$$k[nR, R] \leq Rn - R[\log_2 (n+1)].$$

Then for $N = nR + r, 0 \leq r < R$,

$$\begin{aligned} k[N, R] &\leq k[nR, R] + r \\ &\leq nR + r - R[\log_2 (n+1)] \\ &= N - R\left[\log_2 \left(\left[\frac{N}{R}\right] + 1\right)\right], \end{aligned}$$

$$\begin{aligned} k[N+2, R+1] &\leq N + 2 \\ &\quad - (R+1)\left[\log_2 \left(\left[\frac{N+2}{R+1}\right] + 1\right)\right]. \end{aligned} \tag{69}$$

For R fixed there is an N_0 such that, for $N \geq N_0$,

$$\left\{\frac{N+2}{2(R+1)}\right\}^{R+1} \geq 4 \sum_{i=0}^{R} \binom{N}{i}.$$

This implies

$$(R+1)\left[\log_2 \left(\left[\frac{N+2}{R+1}\right] + 1\right)\right] \geq \log_2 \left\{4 \sum_{i=0}^{R} \binom{N}{i}\right\}. \tag{70}$$

But from (1),

$$K(N, R) \geq \frac{2^N}{\sum_{i=0}^{R} \binom{N}{i}}, \tag{71}$$

and (68) follows from (69)–(71).

We now consider the cases $R = 1$ and 2 in more detail.

Theorem 34: For $n = 2, 3, \cdots, 8, 10, 11, \cdots, 15$ and $n \geq 28$,

$$K(n+2, 2) \leq K(n, 1). \tag{72}$$

Proof: From (70), (72) holds provided

$$2c \geq 2 + \log_2 (n+1) \tag{73}$$

where

$$c = \left[\log_2 \left(\left[\frac{n}{2}\right] + 2\right)\right].$$

Now $2^{c+1} - 4 \leq n \leq 2^{c+2} - 5$. Thus, for n varying between $2^{c+1} - 4$ and $2^{c+2} - 5$, we have

$$2 + \log_2 (n+1) \leq 2 + \log_2 (2^{c+2} - 4) \leq 4 + c.$$

For $c \geq 4$ ($n \geq 28$), $2 + \log_2 (n+1) \leq 4 + c \leq 2c$, and (73) holds. For $c = 3$ ($12 \leq n \leq 27$), (73) holds if $12 \leq n \leq 15$. For $c = 1$ or 2 ($1 \leq n \leq 11$), (73) does *not* hold, but (72) is nevertheless true for $n = 2, 3, \cdots, 8, 10, 11$ from Table I. This completes the proof.

Theorem 35: For $n = 1, 3, 4, 5, 6, 7; 43, 44; 91, 92, \cdots, 127; 187, 188, \cdots, 361$; and $n \geq 379$,

$$K(n+2, 3) \leq K(n, 2).$$

We omit the proof, which may be found in [16].

VI. Density of a Covering

In this final section we study the analog of conjectures B and C for codes over general alphabets. For this purpose it is convenient to introduce the density of a covering. Let C be an additive code of length n and covering radius R over the cyclic group Z_q of q elements (q need not be a prime power). Let $K^*(n, R, q)$ denote the minimal number of codewords in such a code, and $K(n, R, q)$ the corresponding quantity for arbitrary (i.e. not necessarily additive) subsets of Z_q^n. In particular, $K(n, R, 2) = K(n, R)$. The *density* of C is defined to be

$$\mu^*(n, R, q) = K^*(n, R, q) \cdot q^{-n} \sum_{i=0}^{R} (q-1)^i \binom{n}{i} \tag{74}$$

(with a similar definition for $\mu(n, R, q)$). Thus $\mu^* \geq 1$, with $\mu^* = 1$ if and only if C is a perfect code.

By taking direct sums we have

$$\begin{aligned} &K^*(n_1 + n_2, R_1 + R_2, q) \\ &\qquad \leq K^*(n_1, R_1, q) K^*(n_2, R_2, q). \end{aligned} \tag{75}$$

Mauldon [22] shows that for $q = p =$ prime,

$$K^*(n, 1, p) = p^{n-r} \tag{76}$$

where r is defined by

$$p^r \leq n(p-1) + 1 < p^{r+1}. \tag{77}$$

Theorem 36: For a fixed prime p and fixed R, for sufficiently large n there exist additive codes with density $\mu^*(n, R, p)$ independent of n.

Remarks: This seems to be the best result presently known. Wyner and Ziv [34] obtain $\mu(n, R, p) = o(p^n)$, Lovász [19] has $\mu(n, R, p) \approx O(R \log n)$, and [3], [4] give $\mu^*(n, R, p) = O(n^2)$.

Proof: From (76),

$$K^*(n,1,p) \le \frac{p^n}{1+n(p-1)}p, \tag{78}$$

so, from (75),

$$K^*(Rn,R,p) \le \frac{p^{nR+R}}{(1+n(p-1))^R}. \tag{79}$$

Therefore

$$\mu^*(Rn,R,p) \le \frac{p^R \sum_{i=0}^{R}(p-1)^i\binom{nR}{i}}{(1+n(p-1))^R},$$

which, using standard methods (e.g., [20, ch. 10, sec. 11]), may be bounded above by

$$\frac{(R+1)(Rp)^R}{R!} \sim \sqrt{\frac{R}{2\pi}}(pe)^R(1+o(1))$$

as $N = Rn \to \infty$, as claimed.

We now generalize Theorem 36 to all q.

Lemma 37:

$$K^*(n,1,rs) \le s^{n-1}K^*(n,1,r).$$

Stanton *et al.* [27] prove Lemma 37 for nonadditive codes, and the same proof holds for additive codes.

Theorem 38: For any fixed q and R, for sufficiently large n there exist additive codes with density $\mu^*(n,R,q)$ independent of n.

Proof: Case 1) $q = p^m$. From Lemma 37 and (78),

$$\begin{aligned} K^*(n,1,p^m) &= K^*(n,1,p^{m-1}\cdot p) \\ &\le p^{(m-1)(n-1)}K^*(n,1,p) \\ &\le \frac{p^{mn-m+2}}{1+n(p-1)}. \end{aligned} \tag{80}$$

This implies $\mu^*(n,1,p^m) \le p+2$ for n sufficiently large. From (75) and (80),

$$K^*(nR,R,p^m) \le \left\{\frac{p^{mn-m+2}}{1+n(p-1)}\right\}^R$$

which implies

$$\mu^*(N,R,p^m) \le \sqrt{\frac{R}{2\pi}}\{(p+2)e\}^R(1+o(1))$$

as $N \to \infty$.

Case 2) $q = p_1^{m_1}p_2^{m_2}$. Again using Lemma 37 and (78), we obtain

$$K^*(n,1,p_1^{m_1}p_2^{m_2}) \le \left(p_1^{m_1}p_2^{m_2-1}\right)^{n-1}\frac{p_2^{n+1}}{1+n(p_2-1)}$$

which implies

$$\mu^*(n,1,p_1^{m_1}p_2^{m_2}) \le p_2+2, \qquad n \to \infty,$$

and therefore

$$\mu^*(n,1,p_1^{m_1}p_2^{m_2}) \le \min(p_1+2, p_2+2), \qquad n \to \infty.$$

Then (75) leads to

$$\mu^*(N,R,p_1^{m_1}p_2^{m_2}) \le \sqrt{\frac{R}{2\pi}}\{e\cdot\min(p_1+2,p_2+2)\}^R(1+o(1))$$

with a similar result in the general case.

Corollary 39: For q and R fixed, and n sufficiently large,

$$K^*(n+2,R+1,q) \le K^*(n,R,q)$$

and

$$K(n+2,R+1,q) \le K(n,R,q).$$

Proof: This is a consequence of

$$K(n+2,R+1,q) \le K^*(n+2,R+1,q) \le O\left(\frac{q^{n+2}}{n^{R+1}}\right)$$

(Theorem 38) and

$$K^*(n,R,q) \ge K(n,R,q) \ge O\left(\frac{q^n}{n^R}\right)$$

(the sphere bound).

Note Added in Proof

For further results see N. J. A. Sloane, "A new approach to the covering radius of codes," *J. Cobin. Theory*, Ser. A, vol. 42, pp. 61–86, 1986; K. E. Kilby and N. J. A. Sloane, "On the covering radius problem for codes: (I) Bounds on normalized covering radius," *Siam J. Algeb. Discr. Methods*, to appear; and K. E. Kilby and N. J. A. Sloane, "On the covering radius problem for codes: (II) Codes of low dimension; normal and abnormal codes,: *Siam J. Algeb. Discr. Methods*, to appear.

Acknowledgments

We are grateful to R. L. Graham and A. M. Odlyzko for suggestions that led to Lemma 21 and Theorem 2 respectively. We also thank the referees for some helpful comments.

References

[1] T. Berger, *Rate Distortion Theory*. Englewood Cliffs, NJ: Prentice-Hall, 1971.
[2] M. R. Best, "Binary codes with a minimum distance of four," *IEEE Trans. Inform. Theory*, vol. IT-26, pp. 738–742, 1980.
[3] G. D. Cohen, "A nonconstructive upper bound on covering radius," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 352–353, 1983.
[4] G. Cohen and P. Frankl, "Good coverings of Hamming spaces with spheres," *Discrete Math.*, vol. 56, pp. 125–131, 1985.
[5] G. D. Cohen, M. R. Karpovsky, H. F. Mattson, Jr., and J. R. Schatz, "Covering radius: Survey and recent results," *IEEE Trans. Inform. Theory*, vol. IT-31, pp. 328–343, May 1985.

[6] G. D. Cohen, A. C. Lobstein, and N. J. A. Sloane, "On a conjecture concerning coverings of Hamming space," in *Proc. Int. Conf. Algebra, Algorithms and Codes, Toulouse, France, 1984.* New York: Springer-Verlag, 1986, to appear.
[7] T. J. Dickson, "On a covering problem concerning Abelian groups," *J. London Math. Soc.*, vol. 3, pp. 222–232, 1971.
[8] H. Fernandes and E. Rechtschaffen, "The football pool problem for 7 and 8 matches," *J. Comb. Theory*, Ser. A., vol. 35, pp. 109–114, 1983.
[9] T. J. Goblick, Jr., "Coding for a discrete information source with a distortion measure," Ph.D. dissertation, Elec. Eng. Dep. Mass. Inst. Technol., Cambridge, 1962.
[10] R. L. Graham and N. J. A. Sloane, "On the covering radius of codes," *IEEE Trans. Inform. Theory*, vol. IT-31, pp. 385–401, May 1985.
[11] H. J. Helgert and R. D. Stinaff, "Minimum-distance bounds for binary linear codes," *IEEE Trans. Inform. Theory*, vol. IT-19, pp. 344–356, 1973.
[12] J. G. Kalbfleisch and R. G. Stanton, "A combinatorial problem in matching," *J. London Math. Soc.*, vol. 44, pp. 60–64, 1969; and vol. 1, p. 398, 1969.
[13] J. G. Kalbfleisch, R. G. Stanton, and J. D. Horton, "On covering sets and error-correcting codes," *J. Combin. Theory*, vol. 11, pp. 233–250, 1971.
[14] H. J. L. Kamps and J. H. van Lint, "The football pool problem for 5 matches," *J. Combin. Theory*, vol. 3, pp. 315–325, 1967.
[15] G. L. Katsman and S. N. Litsyn, personal communication.
[16] A. C. Lobstein, "Contributions au codage combinatoire: Ordres additifs, rayon de recouvrement," Thèse de docteur-ingénieur, École Nationale Supérieure des Télécommunications, Paris, France, 1985.
[17] A. Lobstein, G. Cohen, and N. J. A. Sloane, "Recouvrements d'espaces de Hamming binaires," *Comptes Rendus Acad. Sci.*, Series I, vol. 301, pp. 135–138, 1985.
[18] G. O. Losey, "Note on a theorem of Zaremba," *J. Combin. Theory*, vol. 6, pp. 208–209, 1969.
[19] L. Lovász, "On the ratio of optimal integral and fractional covers," *Discrete Math.*, vol. 13, pp. 383–390, 1975.
[20] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes.* Amsterdam: North-Holland, 1977.
[21] E. Mattioli, "Sopra una particolare proprieta dei gruppi abeliani finiti," *Ann. Scuola Norm. Sup. Pisa*, vol. 3, pp. 59–65, 1950.
[22] J. G. Mauldon, "Covering theorems for groups," *Quart. J. Math. Oxford Ser.*, vol. 1, pp. 284–287, 1950.
[23] M. Mollard, "Les invariants du n-cube," Thesis, Univ. de Grenoble, France, 1981.
[24] A. M. Romanov, "New binary codes of minimal distance 3" (in Russian), *Problemy Peredachi Informatsii*, vol. 19, no. 3, pp. 101–102, 1983.
[25] N. J. A. Sloane and D. S. Whitehead, "A new family of single-error-correcting codes," *IEEE Trans. Inform. Theory*, vol. IT-16, pp. 717–719, 1970.
[26] R. G. Stanton, "Covering theorems in groups (or: how to win at football pools)," in *Recent Progress in Combinatorics*, W. T. Tutte, Ed., New York: Academic, 1969, pp. 21–36.
[27] R. G. Stanton, J. D. Horton, and J. G. Kalbfleisch, "Covering theorems for vectors with special reference to the case of four and five components," *J. London Math. Soc.*, vol. 1, pp. 493–499, 1969.
[28] R. G. Stanton and J. G. Kalbfleisch, "Covering problems for dichotomized matchings," *Aequationes Math.*, vol. 1, pp. 94–103, 1968.
[29] ——, "Intersection inequalities for the covering problem," *SIAM J. Appl. Math.*, vol. 17, pp. 1311–1316, 1969.
[30] O. Taussky and J. Todd, "Covering theorems for groups," *Ann. Soc. Polon. Math.*, vol. 21, pp. 303–305, 1948.
[31] ——, "Some discrete variable computations," in *Proc. Symp. Appl. Math.*, vol. 10. Providence, RI. Amer. Math. Soc., 1960, pp. 201–209.
[32] A. Tietäväinen, "Bounds for binary codes just outside the Plotkin range," *Inform. Contr.*, vol. 47, pp. 85–93, 1980.
[33] E. W. Weber, "The football pool problem for 6 matches: A new upper bound," *J. Combin. Theory*, Ser. A, vol. 35, pp. 106–108, 1983.
[34] A. D. Wyner and J. Ziv, "On communication of analog data from a bounded source space," *Bell Syst. Tech. J.*, vol. 48, pp. 3139–3172, 1969 (see p. 3168, Lemma 2).
[35] S. K. Zaremba, "A covering theorem for Abelian groups," *J. London Math. Soc.*, vol. 26, pp. 71–72, 1950.
[36] ——, "Covering problems concerning Abelian groups," *J. London Math. Soc.*, vol. 27, pp. 242–246, 1952.