On the Covering Radius of Codes*

R. L. Graham
N. J. A. Sloane

Bell Laboratories
Murray Hill, NJ 07974

I. Introduction

Designing a good error-correcting code is a *packing* problem. The corresponding *covering* problem has received much less attention: now the codewords must be placed so that no vector of the space is very far from the nearest codeword. The two problems are quite different, and with a few exceptions good packings, i.e. codes with a large minimal distance, are usually not especially good coverings. The recent survey of Cohen, Karpovsky, Mattson and Schatz [8] gives an excellent summary of earlier work, as well as a number of new results. (A recent Soviet paper [19], not mentioned in [8], studies codes of very high rate.)

In the present paper we address two of the central problems: the mathematical question of determining $t[n, k]$, the smallest covering radius of any $[n, k]$ binary linear code, and the more practical problem of constructing codes having a specified length and dimension and with a reasonably small covering radius. We call such codes *covering codes* (in contrast to *error-correcting codes*).

In order to have a standard by which to judge new codes, we give a table of bounds on $t[n, k]$ for $n \leq 64$. This is more extensive than the table in [8], which is for $n \leq 32$;

* This appeared in ‘‘IEEE Trans. Information Theory’’, vol. 31 (1985), pp. 385–401.

furthermore many of the entries in that table have now been improved.

A number of the results in [8] are obtained by taking direct sums of codes. One of the themes of the present paper is that *direct sums can usually be improved*. In order to describe the new constructions we introduce a quantity called the *norm* of a code (defined in Section II). Usually the norm is $\leq 2R+1$, where R is the covering radius, in which case the code is called *normal*.

The simplest and most powerful of the new constructions is the following. If $C^{(1)}$ is an $[n_1, k_1]$ code with covering radius R_1, or in short an $[n_1, k_1]\ R_1$ code, and $C^{(2)}$ is an $[n_2, k_2]\ R_2$ code, then their direct sum [18, p. 76] $C^{(1)} \oplus C^{(2)}$ is an $[n_1 + n_2, k_1 + k_2]\ R_1 + R_2$ code. But if $C^{(1)}$ and $C^{(2)}$ are normal, then we may form their *amalgamated direct sum*, which is an

$$[n_1 + n_2 - 1, k_1 + k_2 - 1]\ R_1 + R_2$$

code (Theorem 19). This has one fewer coordinate than the direct sum, but the same covering radius and the same redundancy. The construction is described pictorially in Figure 1(d).

In particular, since the trivial [3,1] $R = 1$ code $\{000, 111\}$ is normal (by Theorem 3), we can extend any $[n, k]\ R$ normal code to an $[n+2, k]\ R+1$ normal code. In this way, if we can find a good covering code to begin with, we can move horizontally across the $t[n, k]$ table in steps of 2, only increasing the covering radius by 1 at each step (Theorem 20). This has enabled us to determine $t[n,4]$ and $t[n,5]$ exactly (Theorems 21 and 22), and to obtain the general upper bound on $t[n, k]$ given in Theorem 24. A matching lower bound is given in Theorem 26, and a conjecture for the true value of

$t[n, k]$ for fixed k and large n is given in (50), (51).

We believe that there are many codes which are not normal, although at the present time we do not have a single example. Since normal codes are essential for the amalgamated direct sum construction, Section II is devoted to their study.

The amalgamated direct sum construction and its applications are described in Section III. In some cases it is possible to obtain a further improvement over the simple direct sum, and to save not just one but two or even more coordinates. These constructions are described in Section IV. We then use these results to study the special case of codes with covering radius 2. (Covering radius 1 is easily handled using Hamming codes and the sphere bound.) For given length n, let k^* be the smallest dimension of any code with covering radius 2. In Theorem 30 we determine k^* to within at most 2, for any value of n.

In general it is extremely difficult to find the covering radius of a large code, or even to estimate it. Section V describes another way of improving on the direct sum, the *extended direct sum*, which produces infinite sequences of codes, of any specified rate, for which it is possible to give a reasonably good upper bound on the covering radius. The structure of these codes is displayed in Figure 5.

The final section of the paper gives the main table of $t[n, k]$, and a list of ''seeds,'' codes from which all others in the table can be derived by one of the constructions. There are surprisingly few seeds. Most of the codes in the table are obtained either by a trivial modification of an earlier code using the rules (86)-(88) (for example, taking the direct sum with $\{0,1\}$), or by applying Theorem 20, using rule (89). Because such codes

are not always satisfactory for applications, we have mentioned alternative constructions in several places (see (79), (81), (85), (91) and (92) for example). The paper ends with a short list of open problems.

One of our reasons for investigating this problem was a question raised by our colleagues B. S. Atal and M. R. Schroeder in connection with the efficient coding of speech [1]-[3]: what is the best way to place M points ''uniformly'' on the surface of a sphere in n-dimensional Euclidean space? 256 points on a 64-dimensional sphere, for example? Such questions seem very difficult, but if $M \leq 2^n$ an approximate solution can be obtained by taking the points to be the codewords of a good covering code (since the vertices of a unit cube lie on the surface of the circumscribing sphere).

In this paper all codes are linear and binary, i.e. are defined over $\mathbf{F}_2 = \{0,1\}$.

II. Normal Codes

Definitions. Let C be a binary linear code of length n, dimension k and covering radius R, i.e. an $[n, k]$ R code. If i is any one of the n coordinates, let $C_0^{(i)}$ denote the set of codewords in which the i-th coordinate is 0, and $C_1^{(i)}$ the codewords in which it is 1. We assume that $C_1^{(i)}$ is non-empty, and so both $C_0^{(i)}$ and $C_1^{(1)}$ contain 2^{k-1} codewords [16, p. 13]. For any binary n-tuple x, let

$$f_0(x) = \mathrm{dist}(x, C_0^{(i)}) = \min_{c \in C_0^{(i)}} \mathrm{dist}(x, c) ,$$

$$f_1(x) = \mathrm{dist}(x, C_1^{(i)}) .$$

Then

$$N^{(i)} = \max_x \{ f_0(x) + f_1(x) \} \tag{1}$$

is called the *norm of C with respect to the i-th coordinate, and*

$$N = \min_i N^{(i)} \tag{2}$$

is the *norm* of C. Coordinates i for which $N = N^{(i)}$ are called *acceptable*. Finally, a code is *normal* if its norm satisfies

$$N \leq 2R+1 \ . \tag{3}$$

Remarks. (i) In other words, if a code has norm N, then there is a coordinate i such that, for any vector x, the sum of the distances from x to the nearest codeword with a 0 in the i-th place, and to the nearest codeword with a 1 in the i-th place, is at most N (and for some x this sum is equal to N).

(ii) When testing (2), it is enough to consider vectors x which are coset representatives for C, i.e. are distinct modulo C (since $f_0(x+c) + f_1(x+c) = f_0(x) + f_1(x)$ for all $c \in C$). In particular it is enough to test vectors x of weight $\leq R$.

Examples

(a) The code $C = \{000, 111\}$. All coordinates are clearly equivalent and we have $C_0^{(1)} = \{000\}$, $C_1^{(1)} = \{111\}$. If $x = 000$, $f_0 = 0$ & $f_1 = 3$; if $x = 100$, $f_0 = 1$ & $f_1 = 2$. This is enough (by the previous remark) to show that C has norm $N = 3$, and all coordinates are acceptable. Since C has covering radius $R = 1$, C is normal.

(b) $C = \{00000, 11000, 00111, 11111\}$, $R = 2$. Working with respect to the first coordinate, $C_0^{(1)} = \{00000, 00111\}$, $C_1^{(1)} = \{11000, 11111\}$, and we have

x	f_0	f_1
00000	0	2
10000	1	1
00100	1	3
10100	2	2
00110	1	3

This is enough to show that C has norm $N = 4$ and therefore is normal. The first two coordinates are acceptable. However, the last three coordinates are unacceptable. Taking $i = 3$, for example, and $x = 10100$, we find $f_0 = 2$, $f_1 = 3$ and $N^{(3)} = 5$, violating (2).

(c) This is an interesting example of an indecomposable code in which not every coordinate is acceptable. (It has also been a useful source of counterexamples for various conjectures.) This code has parameters [10,5] $R = 2$, and is defined by the generator matrix (4).

$$\left[\begin{array}{c|c} 1\,0\,0\,0\,0 & 1\,1\,1\,1\,0 \\ 0\,1\,0\,0\,0 & 1\,0\,0\,0\,1 \\ 0\,0\,1\,0\,0 & 0\,1\,0\,0\,1 \\ 0\,0\,0\,1\,0 & 0\,0\,1\,0\,1 \\ 0\,0\,0\,0\,1 & 0\,0\,0\,1\,1 \end{array}\right] \qquad (4)$$

Working with respect to the first coordinate, we find that when $x = 00...01$, $f_0 = 1$ & $f_1 = 5$. On the other hand the norm is 5 with respect to the other nine coordinates, and so the code is normal, with one unacceptable coordinate.

Remark (iii) It is possible to check the latter assertion by hand, since by Remark (ii) we need only consider vectors x of weights 0, 1 and 2. For larger codes, however, it is essential to have a computer program to do the checking. In the course of this investigation we have made extensive use of computers, for exploratory work (searching

for codes with low covering radius), for analyzing specific codes (computing the covering radius and norm), and for showing that certain codes do not exist (see Theorem 22 below). The programs were all fairly straightforward, although it is worth mentioning that we found the algorithms in Nijenhaus and Wilf [21] useful for generating all k-subsets of an n-set, for example.

Before considering specific families of codes, we first give some general results.

Theorem 1. (i) *A code of norm N has covering radius*

$$R \le \left\lceil \frac{N}{2} \right\rceil . \tag{5}$$

(ii) *For a normal code,*

$$N = 2R \quad or \quad 2R+1 . \tag{6}$$

(iii) *If a code is even* (*i.e. the weight of every codeword is even*), *N is even. In particular if a code is even and normal,* $N = 2R$.

Example (b) above shows that N can be even, even if the code is not.

Proof. (i) For any vector x,

$$\begin{aligned} \mathrm{dist}(x, C) &= \min \{ f_0(x), f_1(x) \} \\ &\le \frac{1}{2}(f_0(x) + (f_1(x)) \le \frac{1}{2} N . \end{aligned} \tag{7}$$

(ii) Let x be at distance R from C. Then $f_0(x) \ge R$, $f_1(x) \ge R$, and so $N^{(i)} \ge 2R$, for all i. Therefore $N \ge 2R$, for any code, and if C is normal, $2R \le N \le 2R+1$. (iii) If C is even, $f_0(x)$ and $f_1(x)$ are always both even or both odd, and so all $N^{(i)}$ are even.

The next theorem expresses the norm in terms of a parity check matrix for the code, which is sometimes more convenient.

Theorem 2. *Let H be a parity check matrix for a code C with parameters $[n, k]$ R, and let i be a coordinate at which the code is nonzero. For any binary $(n-k)$-tuple s, let $h_0(s)$ be the minimal number of columns of H which add to s, not using the i-th column, and let $h_1(s)$ be the minimal number which add to s, when the i-th column must be used. Then*

$$N^{(i)} = \max_s \{h_0(s) + h_1(s)\} , \tag{8}$$

and C has norm N if and only if, for some coordinate i,

$$\max_s \{h_0(s) + h_1(s)\} = N . \tag{9}$$

This is analogous to the result that a code has covering radius R if and only if every $(n-k)$-tuple s can be written as the sum of at most R columns of H [8, (1.2.2)].

Proof. For $j = 0, 1$, let

$$g_j(x) = \min_{c \in C} \{\mathrm{wt}(x+c) : \text{the } i\text{-th coordinate of } x+c \text{ is equal to } j\} . \tag{10}$$

If the i-th coordinate of x is 0, $f_0(x) = g_0(x)$ and $f_1(x) = g_1(x)$, while if the i-th coordinate of x is 1, $f_0(x) = g_1(x)$ and $f_1(x) = g_0(x)$. In either case $f_0(x) + f_1(x) = g_0(x) + g_1(x)$. Thus

$$N^{(i)} = \max_x \{g_0(x) + g_1(x)\} . \tag{11}$$

The syndrome of x is $s = Hx^{tr}$, and s is equal to the sum of those columns of H where $x+c$ is 1, for any choice of $c \in C$ [18, p. 17]. Therefore $g_0(x) = h_0(s)$,

$g_1(x) = h_1(s)$. The desired result now follows from (11).

Although we believe that many codes are not normal, we have not yet found an example of such a code. We now describe several families of codes which are normal.

Theorem 3. *The repetition code* $\{0^n, 1^n\}$*, the code consisting of all vectors of length n of even weight, and the code consisting of all vectors of length n are normal* (*and every coordinate is acceptable*).

We omit the easy proof. In future, if the automorphism group of a normal code is transitive on the coordinates, we shall omit the obvious remark that all coordinates are acceptable.

Lemma 4. (i) *Adding a column to a generator matrix for a code can increase the norm by at most* 2. (ii) *If the code is normal, and the covering radius is increased by this operation, the new code is also normal.*

Proof. (i) Suppose C has covering radius R, norm N, and the first coordinate (say) is acceptable. We use primes to refer to the new code. Working with respect to the first coordinate, if $x' = (x, \varepsilon)$, $\varepsilon = 0$ or 1, we have

$$f_0'(x') \le f_0(x) + 1 , \quad f_1'(x') \le f_1(x) + 1 ,$$

$N^{(1)'} \le N^{(1)} + 2$, and $N' \le N+2$. (ii) If C is normal and C' has covering radius $R' = R+1$, then $2R' + 1 = 2R + 3 \ge N+2 \ge N'$, as required.

Theorem 5. *If C is normal then so is* (i) *any code obtained by appending any number of* 0*'s to the codewords of C, and* (ii) *the code obtained by appending an overall parity check to C, if C contains any codeword of odd weight.*

Proof. Immediate from Lemma 4, since these operations increase the covering radius of C [8, (3.7.2)].

The following converse to (ii) will be needed for the proof of Theorem 24.

Theorem 6. *Suppose C is even and has norm N. Deleting any nonzero coordinate* (*provided at least one of the originally acceptable coordinates remains*) *produces a code C' of norm $N-1$. In particular if C is normal, so is C'.*

Proof. Suppose C is an $[n, k]$ R code. Then C' has covering radius $R-1$ (*cf.* [8, (3.7.2)]). By Theorem 1, N is even, say $N = 2M$. For concreteness let us suppose that the first coordinate of C is acceptable, and the last coordinate is deleted to produce C'. We must show that $N^{(1)'} \leq 2M-1$.

Let x be any vector of length $n-1$, and let $X = (x,0)$. Let c_i be a closest codeword to X in $C_i^{(1)}$ $(i = 0, 1)$. Then, from (2),

$$\text{dist}(c_0, X) + \text{dist}(c_1, X) \leq 2M .$$

If either c_0 or c_1 ends with 1 then the shortened vectors c_0', c_1' satisfy

$$\text{dist}(c_0', x) + \text{dist}(c_1', x) \leq 2M-1 ,$$

as required. So we may assume that

$$\text{all } c_0' \text{ and } c_1' \text{ have even weight .} \tag{12}$$

Let $c = (c',0)$ denote the closer of c_0, c_1 to X, and let $d = \text{dist}(c', x)$.

Consider $Y = (x,1)$. One candidate for a closest vector to Y is c, at distance $d+1$. Could there be anything closer, say $b = (b', \varepsilon)$, with $\text{dist}(b, Y) \leq d$? Clearly $\varepsilon = 1$,

or else b' is too close to x. But now b is a possible choice for c_0 or c_1, contradicting (12). Therefore no codeword of C is closer to Y than c is. There are now two cases. (a) If $c \in C_0^{(1)}$, then since C has norm $2M$ there is an $a \in C_1^{(1)}$ with

$$\text{dist}(a, Y) \leq 2M - d - 1 ,$$

and the shortened codewords c', a' satisfy $c' \in C_0^{(1)'}$, $a' \in C_1^{(1)'}$ and

$$\text{dist}(c', x) + \text{dist}(a', x) \leq 2M - 1 ,$$

as required. (b) If $c \in C_1^{(1)}$, a similar argument completes the proof.

Theorem 7. *Let C have covering radius R and minimal distance d, and suppose the codewords of weight d form a t-design* [18, p. 58]. *If $R + 1 \leq t$, the code is normal.*

Proof. It is easy to see that, for any code, the minimal distance d and covering radius R are related by

$$d \leq 2R + 1 . \tag{13}$$

We shall show that the first coordinate is acceptable. By Remark (iii) above it is enough to consider vectors x of weight $w \leq R$. First suppose x begins with 0. By the t-design property there is a codeword $c \in C_1^{(1)}$ of weight d having 1's in the first coordinate and also where x is 1, so that $\text{dist}(x, c) = d - w$. Then $f_0(x) \leq w$, $f_1(x) \leq d - w$, and $f_0(x) + f_1(x) \leq d \leq 2R + 1$ by (13). A similar argument applies when x begins with 1. Thus $f_0(x) + f_1(x) \leq 2R + 1$ for all x, and C has norm $\leq 2R + 1$.

Corollary 8. *Hamming codes, extended Hamming codes, and the perfect and extended perfect Golay codes of lengths 23 and 24 are normal.*

Proof. The parameters of the associated t-designs may be found, for example, in [18, pp. 63,67].

Theorem 9. *Let B be an $[n_1, k_1]$ R_1 code with norm N_1, and C an $[n_2, k_2]$ R_2 code with norm N_2. The direct sum $B \oplus C$ has covering radius $R_1 + R_2$ and norm*

$$N = min \{N_1 + 2R_2 , N_2 + 2R_1\} . \tag{14}$$

The direct sum of two normal codes is normal.

Example (b) above illustrates this theorem.

Proof. Working with respect to an acceptable coordinate for B we have

$$f_0(x,y) = f_0^B(x) + \min \{f_0^C(y) , f_1^C(y)\} ,$$
$$f_1(x,y) = f_1^B(x) + \min \{f_0^C(y) , f_1^C(y)\} ,$$

using an obvious notation, so

$$\max_{x,y} \{f_0(x,y) + f_1(x,y)\} = N_1 + 2R_2 .$$

On the other hand, working with respect to an acceptable coordinate for C, we have

$$\max_{x,y} \{f_0(x,y) + f_1(x,y)\} = N_2 + 2R_1 .$$

Therefore $B \oplus C$ has norm equal to $\min \{N_1 + 2R_2 , N_2 + 2R_1\}$. If B and C are normal then $N_1 + 2R_2 \le (2R_1 + 1) + 2R_2 = 2(R_1 + R_2) + 1$, and similarly for $N_2 + 2R_1$, implying that $B \oplus C$ is normal.

Theorem 10. *For a code in which no coordinate is identically zero, we have*

$$norm \le length . \tag{15}$$

Proof. For any i, and $j = 0$ or 1,

$$f_j(x) \le \frac{1}{2^{k-1}} \sum_{c \in C_j^{(i)}} \mathrm{dist}(x,c) ,$$

$$f_0(x) + f_1(x) = \frac{1}{2^{k-1}} \sum_{c \in C} \mathrm{dist}(x,c) = n ,$$

so the norm $N \le n$.

(This is similar to the proof that a code of this type has covering radius $R \le n/2$ given in [16, Theorem 2].)

Theorem 11. *Any code of dimension* 1 *or* 2 *is normal, and every coordinate is acceptable.*

Proof. The result for dimension 1 follows from Theorems 3 and 5. Suppose C has dimension 2. By Theorem 5 we can assume there is no zero coordinate, and so the four codewords of C have this form:

$$\begin{array}{ccc} 0\,0\,..\,0 & 0\,0\,..\,0 & 0\,0\,..\,0 \\ 0\,0\,..\,0 & 1\,1\,..\,1 & 1\,1\,..\,1 \\ 1\,1\,..\,1 & 0\,0\,..\,0 & 1\,1\,..\,1 \\ 1\,1\,..\,1 & 1\,1\,..\,1 & 0\,0\,..\,0 \end{array}$$

with respectively a,b,c coordinates of the three types, where $a+b+c = n$. It is not difficult to show that the covering radius of this code is

$$R = \left\lceil \frac{a}{2} \right\rceil + \left\lceil \frac{b}{2} \right\rceil + \left\lceil \frac{c}{2} \right\rceil , \tag{16}$$

unless all of a,b,c are odd, in which case

$$R = \left\lceil \frac{a}{2} \right\rceil + \left\lceil \frac{b}{2} \right\rceil + \left\lceil \frac{c}{2} \right\rceil + 1 \ . \tag{17}$$

We omit the proof. If a,b,c are all even, then $R = n/2$ from (16), $2R+1 = n+1$, and C is normal by Theorem 10. Similarly in the case when a,b,c are all odd, or when precisely one of them is odd. The difficult case occurs when precisely two of a,b,c are odd, so that $R = \frac{1}{2}\, n-1$, $2R+1 = n-1$. Consider an arbitrary vector

$$x = 0\,.\,.\,0\ 1\,.\,.\,1 \quad 0\,.\,.\,0\ 1\,.\,.\,1 \quad 0\,.\,.\,0\ 1\,.\,.\,1$$

with i 1's in the a coordinates, j 1's in the b coordinates, and k 1's in the c coordinates. Then

$$f_0(x) = i + \min\{j+k,\ (b+c) - (j+k)\}\ ,$$
$$f_1(x) = a-i + \min\{b-(j-k),\ c+(j-k)\}\ .$$

Replacing the minima by their averages we obtain

$$f_0(x) + f_1(x) \le a + \frac{b+c}{2} + \frac{b+c}{2} = n\ ,$$

with equality if and only if

$$j+k = (b+c) - (j+k)\ ,$$
$$b-(j-k) = c + (j-k)\ .$$

But these equations imply $b = 2j$, $c = 2k$, contradicting our assumption that two of a,b,c are odd. Therefore $f_0(x) + f_1(x) \le n-1$, and the code has norm $\le n-1$, as required.

Theorem 12. *Any code of length* ≤ 8 *is normal, and every coordinate is acceptable.*

Proof. From Theorems 9 and 11, with extensive computer assistance to deal with the remaining cases.

Theorem 13. *All simplex codes* (*the duals of Hamming codes,* [18, *p.* 30]) *are normal.*

Proof. These codes have parameters $[n = 2^m - 1,\ k = m]$, $R = 2^{m-1} - 1$, and $2R + 1 = n$, so the result follows immediately from Theorem 10.

Next we consider first-order Reed-Muller codes. These codes have parameters $[n = 2^m,\ k = m + 1]$ and covering radius

$$R = \frac{1}{2}\, n - \frac{1}{2}\, \sqrt{n}, \quad \text{if } m \text{ is even}, \tag{18}$$

(Rothaus [25]). For *m* odd it is only known in general that

$$\frac{1}{2}\, n - \sqrt{\frac{n}{2}} \leq R < \frac{1}{2}\, n - \frac{1}{2}\, \sqrt{n} \tag{19a}$$

(see [8] for references), and for odd $m \geq 15$ that

$$\frac{1}{2}\, n - \frac{27}{32}\sqrt{\frac{n}{2}} \leq R < \frac{1}{2}\, n - \frac{1}{2}\sqrt{n} \tag{19b}$$

(Patterson and Wiedemann [22]).

Theorem 14. *The first-order Reed-Muller code of length* $n = 2^m$, $m \geq 1$, *has norm*

$$N \leq n - \sqrt{n}. \tag{20}$$

For even m these codes are normal.

Proof. The second assertion follows from the first using (18). For the first assertion, let *C* be a first-order Reed-Muller code of length $n = 2^m$, $m \geq 1$, and let C_i be the set of

codewords beginning with *i*. We shall use both (0,1)-notation and $(+1,-1)$-notation for vectors. If u is a (0,1) vector, $\tilde{u}$ will denote the corresponding $(+1,-1)$ vector, obtained by changing 1's to -1's and 0's to +1's.

If x is an arbitrary (0,1) vector, $c \in C$, $d(c) = \text{dist}(x, c)$, and

$$\pi(\tilde{c}) = \frac{1}{\sqrt{n}} \tilde{x} \cdot \tilde{c} ,$$

computed as a real inner product, then the familiar relationship between Hamming distance and inner product reads

$$d(c) = \frac{1}{2} n - \frac{1}{2} \sqrt{n}\, \pi(\tilde{c}) . \tag{21}$$

C_1 consists of the binary complements of the vectors of C_0, and so the distances from x to C_1 are determined by the distances to C_0:

$$d(\bar{c}) = n - d(c) , \quad \pi(-\tilde{c}) = -\pi(\tilde{c})$$

(the bar denoting the binary complement). Therefore

$$f_0(x) = \frac{1}{2} n - \frac{1}{2} \sqrt{n} \max_{c \in C_0} \pi(\tilde{c}) ,$$

$$f_1(x) = \frac{1}{2} n + \frac{1}{2} \sqrt{n} \min_{c \in C_0} \pi(\tilde{c}) ,$$

and $f_0(x) + f_1(x) \le n - \sqrt{n}$ will follow if we show

$$\max_{c \in C_0} \pi(\tilde{c}) - \min_{c \in C_0} \pi(\tilde{c}) \ge 2 , \quad \text{for any } x .$$

By symmetry we may assume x begins with 0. Then

$$\sum_{c \in C_0} d(c) = \frac{n(n-1)}{2} , \quad \sum_{c \in C_0} \pi(\tilde{c}) = \sqrt{n} . \tag{22}$$

By Parseval's theorem [25] we have

$$\sum_{c \in C_0} \pi(\tilde{c})^2 = n . \tag{23}$$

Furthermore, since $d(c)$ is an integer, from (21) we can write

$$\pi(\tilde{c}) = \frac{2\gamma(\tilde{c})}{\sqrt{n}} \tag{24}$$

where $\gamma(\tilde{c}) \in \mathbf{Z}$ (the integers).

It is convenient at this point to let $c^{(1)},...,c^{(n)}$ be the codewords of C_0, and to define $y_i = \pi(\tilde{c}^{(i)}) - 1/\sqrt{n}$, for $i = 1,...,n$. From (22)-(24) the y_i are $n = 2^m$ real numbers satisfying

$$\sum_{i=1}^{n} y_i = 0 , \tag{25}$$

$$\sum_{i=1}^{n} y_i^2 = n-1 , \tag{26}$$

$$y_i = \frac{2\gamma_i - 1}{\sqrt{n}} , \quad \gamma_i \in \mathbf{Z} , \tag{27}$$

and we wish to show that

$$\max y_i - \min y_i \geq 2 . \tag{28}$$

Suppose the contrary, and let

$$\max y_i = \frac{2\gamma-1}{\sqrt{n}}\ , \quad a\gamma \in \mathbf{Z}\ , \quad \gamma \geq 0\ ,$$

$$\min y_i = \frac{-2\mu-1}{\sqrt{n}}\ , \mu \in \mathbf{Z}\ , \quad \mu \geq 0\ ,$$

where $\max y_i - \min y_i < 2$, i.e.

$$\mu + \gamma < \sqrt{n} \quad (\mu\ ,\ \gamma \in \mathbf{Z},\ n = 2^m)\ . \tag{29}$$

In fact (29) will force the second moment of the y_i's to be less than $n-1$, violating (26). The largest second moment is obtained when the y_i's are placed at the end-points of their range. If M y_i's are equal to $(-2\mu-1)/\sqrt{n}$, and N are equal to $(2\gamma-1)/\sqrt{n}$, with $M + N = n$, Eq. (25) gives

$$M = \frac{2\gamma-1}{2\gamma+2\mu}\ n\ , \quad N = \frac{2\mu+1}{2\gamma+2\mu}\ n\ .$$

Then $\Sigma\ y_i^2$ simplifies to $(2\gamma-1)(2\mu+1)$, and we will show that (29) implies

$$(2\gamma-1)(2\mu+1) < n-1\ , \tag{30}$$

contradicting (26). Case (i), m even and $\sqrt{n}$ is an integer. Then $\mu + \gamma \leq \sqrt{n} - 1$, from (29), and (30) follows easily. Case (ii), m odd, $m = 2r+1$, $\sqrt{n} = 2^{r+\frac{1}{2}}$. Suppose $\mu+\gamma = k = 2^{r+\frac{1}{2}} - \delta$ with $k \in \mathbf{Z}$, $\delta > 0$. Then (30) reads

$$\mu^2 - \mu(2^{r+\frac{1}{2}} - 1 - \delta) + (2^{2r+1} - 2^{r-\frac{1}{2}} + \frac{\delta}{2}) > 0 \tag{31}$$

which is a quadratic with discriminant

$$k^2 + 1 - 2^{2r+1}\ .$$

Since $k < 2^{r+\frac{1}{2}}$, $k^2 \leq 2^{2r+1} - 1$. So (31) is true unless perhaps the discriminant vanishes. But that would imply $k^2 = 2^{2r+1} - 1$, which is impossible modulo 8 for

$r \geq 1$. Thus the inequality (30) holds in every case, completing the proof of Theorem 14.

We can prove a stronger result when m is 3 or 5.

Theorem 15. *The first-order Reed-Muller codes of length* 8 *and* 32 *are normal.*

Proof. The case $n = 8$ is an extended Hamming code (see Corollary 8), and the case $n = 32$ was verified by computer.

Remark. For every set of parameters $[n, k]$ R for which the main table asserts that a code exists, there is (with at most one exception) a code with the same parameters and norm $2R+1$. The single exception is [59,49] 2, when we have not checked whether the code in Figure 4 is normal.

Whether or not a code C is normal is closely related to the question of how much the covering radius can increase when we consider $C_0^{(1)}$ (the set of codewords beginning with 0) instead of C. The following result leads to an upper bound on the norm of any code, as well as being of some independent interest.

Lemma 16. *Let* C_0 *be any code,* $a \notin C_0$, *and*

$$C = C_0 \cup (a + C_0) .$$

If there is a vector x such that $dist(x, C_0) = r$, *the covering radius of C is at least* $\lceil r/3 \rceil$.

Proof. Let $\text{dist}(C_0, a+C_0) = d$. Then there is a point P (located "midway" between C_0 and $a+C_0$) with

$$\text{dist}(P, C) \geq \left\lceil \frac{d}{2} \right\rceil .$$

On the other hand let c be a closest codeword in $a+C_0$ to x. From the triangle

inequality,

$$\mathrm{dist}(x, c) \geq r - d \ .$$

By taking whichever of x and P is further from C, we see that the covering radius of C is at least

$$\min_d \max \left\{ \left\lceil \frac{d}{2} \right\rceil , \ r - d \right\} ,$$

which is $\geq [r/3]$.

Corollary 17. *If C is any code of covering radius R, then the covering radius of any subcode C_0 of index*$^{(1)}$ *2 is at most* $3R + 2$.

Corollary 18. *If C is any code of covering radius R and norm N, then*

$$2R \leq N \leq 4R + 2 \ . \tag{32}$$

Proof. The left-hand side follows from the proof of Theorem 1 (ii), and the right-hand side from Corollary 17.

III. The Amalgamated Direct Sum Construction

The main reason for studying normal codes is the following construction. Let B be an $[n_1, k_1]$ R_1 code and C an $[n_1, k_2]$ R_2 code. Choose a generator matrix for B which (after permuting the coordinates if necessary) has the form shown in Figure 1(a), and so that the last coordinate, marked with a $(*)$, is acceptable. Similarly choose a generator matrix for C having the form shown in Figure 1(b), and so that the first coordinate is acceptable. Of course the direct sum $B \oplus C$ of these codes is shown in Figure 1(c).

Their *amalgamated direct sum* (or a.d.s., denoted by $B \dot{\oplus} C$) is shown in Figure 1(d). This code has length $n_1 + n_2 - 1$ and dimension $k_1 + k_2 - 1$.

The construction can also be described in terms of parity check matrices. Let H_B be a parity check matrix for B in which the last coordinate is acceptable, and let H_C be a parity check matrix for C in which the first coordinate is acceptable. Then $B \dot{\oplus} C$ is defined by the parity check matrix shown in Figure 1(e). We could also have described the construction in a purely formal way using linear functionals, but we feel these pictorial descriptions are more understandable.

Theorem 19. (i) *The norm of an amalgamated direct sum satisfies*

$$Norm\ (B \dot{\oplus} C) \le Norm\ (B) + Norm\ (C) - 1\ , \tag{33}$$

and the overlapping coordinate is acceptable. (ii) *If B and C are normal then the covering radius of $B \dot{\oplus} C$ is $\le R_1 + R_2$.* (iii) *If B and C are normal and the covering radius of $B \dot{\oplus} C$ is $R_1 + R_2$ then $B \dot{\oplus} C$ is also normal.*

Proof. (i) We use the parity check matrix for $B \dot{\oplus} C$ and apply Theorem 2. For an arbitrary $(n_1 - k_1 + n_2 - k_2)$-tuple $s = \begin{bmatrix} s_1 \\ s_2 \end{bmatrix}$ we have, in an obvious notation,

$$h_0(s) = h_0^B(s_1) + h_0^C(s_2)\ ,$$

while

$$h_1(s) = h_1^B(s_1) + h_1^C(s_2) - 1\ ,$$

since in the latter case the overlapping column is shared by the two codes. Therefore

$h_0(s) + h_1(s) \le N_1 + N_2 - 1$, which establishes (33). (ii) If B and C are normal we have $N_1 \le 2R_1+1$, $N_2 \le 2R_2+1$, so $B \dot{\oplus} C$ has norm $N \le N_1 + N_2 - 1 \le 2(R_1+R_2) + 1$, and covering radius $R \le [N/2] = R_1+R_2$. (iii) Finally, if $R = R_1+R_2$, $N \le 2R+1$.

Examples

(a) Taking B to be the code $\{000, 111\}$ (see example (a) of the previous section), and applying Theorem 19 (iii) we obtain the following. (In this case it is clear that the covering radius of the a.d.s. must be R_1+R_2.)

Theorem 20. (i) *If C is an $[n, k]$ R normal code there are $[n+2i, k]$ $R+i$ normal codes for all $i \ge 0$.* (ii) *If C is an $[n, k]$ code of norm N, there are $[n+2i, k]$ codes of norm $N+2i$ for all $i \ge 0$.*

Generator matrices for these codes are obtained simply by appending 1's to one of the rows of the generator matrix for C (the row associated with an acceptable coordinate), and 0's to all the other rows. For example, the second coordinate in (4) is acceptable, and so the extended codes have generator matrices

1 0 0 0 0	1 1 1 1 0	0 0 0 ... 0
0 1 0 0 0	1 0 0 0 1	1 1 1 ... 1
0 0 1 0 0	0 1 0 0 1	0 0 0 ... 0
0 0 0 1 0	0 0 1 0 1	0 0 0 ... 0
0 0 0 0 1	0 0 0 1 1	0 0 0 ... 0

,

where we have appended $2i$ columns to (4). These codes have a fixed minimal distance, while their covering radius $\to \infty$.

(b) By combining Hamming and Golay codes we obtain

$$[13,7]\ 2 = [7,4]\ 1 \quad a\dot{\oplus} \quad [7,4]\ 1\ , \tag{34}$$

$$[19,10]\ 3 = [13,7]\ 2\dot{\oplus} \quad [7,4]\ 1\ , \tag{35}$$

$$[29,15]\ 4 = [23,12]\ 3\dot{\oplus} \quad [7,4]\ 1\ , \tag{36}$$

and so on. The entries marked with *a* in the main table are obtained in this way.

(c) This example shows that Theorem 19 is false in general if the codes overlap at an unacceptable coordinate. The code with generator matrix

1 1	1 0 0 0 0	1 1 1 1 0
0 0	0 1 0 0 0	1 0 0 0 1
0 0	0 0 1 0 0	0 1 0 0 1
0 0	0 0 0 1 0	0 0 1 0 1
0 0	0 0 0 0 1	0 0 0 1 1

is obtained by overlapping the [3,1] $R = 1$, norm 3 code and the [10,5] $R = 2$, norm 5 code given in (4) at the first (unacceptable) coordinate of the latter code. The new code is a [12,5] $R = 4$, norm 9 code, which satisfies neither (33) nor the conclusion of Theorem 19, part (ii).

Optimal codes of low dimension

Before giving further applications, we first record some elementary properties of the function $t[n, k]$ defined at the beginning of the paper:

$$t[n, k] \le t[n+1, k] \ , \tag{37}$$

$$t[n, k] \ge t[n, k+1] \ , \tag{38}$$

$$t[n, k] \ge t[n+1, k+1] \ . \tag{39}$$

As shown by Cohen *et al*. [8],

$$t[n,1] = \left\lceil \frac{n}{2} \right\rceil , \quad an \ge 1 \ , \tag{40}$$

$$t[n,2] = \left\lceil \frac{n-1}{2} \right\rceil , n \ge 2 \ , \tag{41}$$

$$t[n,3] = \left\lceil \frac{n-2}{2} \right\rceil , n \ge 3 \ . \tag{42}$$

Examples of optimal codes in these three cases (optimal in the sense of having the smallest possible covering radius) are

$$T_n \ , \ \ T_{n-1} \oplus T_1 \ , \ \ T_{n-2} \oplus T_1 \oplus T_1 \ , \tag{43}$$

respectively, where T_n is the repetition code of length *n*.

Theorem 21

$$t[n,4] = \left\lceil \frac{n-4}{2} \right\rceil , \quad for \ n \ne 5 \ , \tag{44}$$

and $t[5,4] = 1$. *Optimal* $[n,4]$ *codes are obtained by applying Theorem* 20 *to the* $[6,4]$ 1 *code* $T_3 \oplus T_1 \oplus T_1 \oplus T_1$ *if n is even, or to the* $[7,4]$ 1 *Hamming code if n is odd.*

Proof. (44) was established for all even *n* in [8], as well as the bound

$t[n,4] \geq [(n-4)/2]$ for all n. On the other hand the codes mentioned (and Theorem 20) show that $t[n,4] \leq [(n-4)/2]$ for $n \geq 6$, completing the proof.

Theorem 22.

$$t[n,5] = \left\lceil \frac{n-5}{2} \right\rceil, \quad \textit{for } n \neq 6 , \tag{45}$$

and $t[6,5] = 1$. *Optimal* $[n,5]$ *codes are obtained by taking the direct sum of the trivial code* $\{0,1\}$ *and an optimal* $[n,4]$ *code.*

Proof. The codes mentioned show that $t[n,5] \leq [(n-5)/2]$ for $n \neq 6$. It remains to establish the lower bounds. The sphere bound (see (56) below) shows that $t[n,5] \geq [(n-5)/2]$ for $n \leq 10$. The Bell Labs Cray-1 computer was used to show that there do not exist codes in which every coordinate is distinct and having any of the following sets of parameters: [11,5] 2, [13,5] 3, [15,5] 4,..., [23,5] 8, [25,5] 9. The total running time was about 41 hours. We now argue as follows (this method of attack was used in [8], although on a much smaller scale, to establish the lower bound of Theorem 21).

Let C be an $[11,5]$ R code. If C contains a repeated coordinate, $R \geq t[9,5] + 1 = 3$; if not the computer proof shows that $R \geq 3$. Thus $t[11,5] \geq 3$, and $t[12,5] \geq 3$ by (37).

Let C be a $[13,5]$ R code. The same reasoning shows $t[13,5] \geq 4$ and $t[14,5] \geq 4$. We repeat this until we have arrived at $t[25,5] \geq 10$ and $t[26,5] \geq 10$.

Let C be a $[27,5]$ R code. If C contains a repeated coordinate then $R \geq t[25,5] + 1 \geq 11$; if not, C is a shortened version of the [31,5] 15 simplex code,

and $R \geq 15-4 = 11$. Therefore $t[27,5] \geq 11$, $t[28,5] \geq 11$. Similarly $t[29,5] \geq 12$, $t[30,5] \geq 12$, $t[31,5] \geq 13$.

For $n \geq 32$ every $[n,5]$ code must contain a repeated coordinate, since there are only 31 distinct nonzero columns for the generator matrix (we need never use a zero coordinate). Therefore $t[n,5] \geq t[n-2,5] + 1$ for $n \geq 32$, which implies $t[n,5] \geq [(n-5)/2]$ for all n, and completes the proof of Theorem 22.

So far only one nontrivial ‘‘seed,’’ the Hamming code of length 7, has been required for generating optimal codes of all dimensions ≤ 5 and any length. At dimension 6 the following more interesting pair of seeds appear.

A [14,6] 3 code, with generator matrix shown in (46).

1 1 1 1 1 1 1 1	1 1 1 0 0 0 0 0 0 0 0 0	0 0 0 1 1 1 0 0 0 0 0 0	0 0 0 0 0 0 1 1 1 0 0 0	0 0 0 0 0 0 0 0 0 1 1 1
1 0 0 1	1 0 0 0 1 0	1 0 0 0 1 0	1 0 0 0 1 0	1 0 0 0 1 0

(46)

This code is normal and every coordinate is acceptable. It has minimal weight 5, and automorphism group of order 48. (Fontaine and Peterson [11] and Helgert [15] have found codes which, although they do not have the simple form of (46), can be shown to be equivalent to this code. It seems likely that there is a unique code with these parameters. If so, this will settle open problem (10.8) of [8], since this code does not contain the all-ones vector.)

A [19,6] 5 code, with generator matrix given in (47).

1	1 1 1 1 1 1	0 0 0 0 0 0	0 0 0 0 0 0
1	0 0 0 0 0 0	1 1 1 1 1 1	0 0 0 0 0 0
1	0 0 0 0 0 0	0 0 0 0 0 0	1 1 1 1 1 1
1	1 1 0 0 0 0	1 1 0 0 0 0	1 1 0 0 0 0
1	0 0 1 1 0 0	0 0 1 1 0 0	0 0 1 1 0 0
0	1 0 1 0 1 0	1 0 1 0 1 0	1 0 1 0 1 0

(47)

This is normal and every coordinate is acceptable. It has minimal weight 7, and automorphism group of order 1152.

By applying Theorem 20 to these two codes, and using (39), we obtain the next result.

Theorem 23.

$$t[n,6] \le \left\lfloor \frac{n-8}{2} \right\rfloor, \quad \textit{afor} \quad n \ge 18 , \tag{48}$$

$$t[n,7] \le \left\lfloor \frac{n-9}{2} \right\rfloor, \textit{for} \quad n \ge 19. \tag{49}$$

Bounds for $t[n,6]$, $t[n,7]$ for $n \le 18$ will be found in the main table. It is worth mentioning that $t[12,6] \ge 3$ was established by computer, and is the only entry in the main table with $k > 5$ where we have been able to improve on the sphere bound.

Inspection of (40)-(42), (44), (45), (48), (49) tempts us to make the following conjecture.

Conjecture. *For all m, there are numbers n_0, n_1 (depending on m) such that*

$$t[n,2m] = \left\lfloor \frac{n-2^m}{2} \right\rfloor, \qquad \textit{afor} \quad n \geq n_0 \ , \tag{50}$$

$$t[n,2m+1] = \left\lfloor \frac{n-2^m-1}{2} \right\rfloor, \textit{for} \quad n \geq n_1 \ . \tag{51}$$

For higher dimensions the best upper bound we have been able to prove is the following.

Theorem 24. *For $m \geq 2$ we have*

$$t[n,2m] \leq \left\lfloor \frac{n - 2^{m-\frac{1}{2}}}{2} \right\rfloor, \qquad \textit{an even} \geq 2^{2m-1} \ , \tag{52}$$

$$t[n,2m] \leq \left\lfloor \frac{n - 2^{m-\frac{1}{2}} - 1}{2} \right\rfloor, n \textit{ odd} \geq 2^{2m-1} - 1 \ , \tag{53}$$

$$t[n,2m+1] \leq \left\lfloor \frac{n - 2^m}{2} \right\rfloor, n \geq 2^{2m} - 1 \ . \tag{54}$$

Proof. For n even we apply Theorem 20 to first-order Reed-Muller codes (using Theorem 14), and for n odd to shortened first-order Reed-Muller codes (using Theorem 6).

Remark. For dimension 8, Theorem 24 yields

$$t[n,8] \leq \left\lfloor \frac{n-12}{2} \right\rfloor, \quad \text{for} \quad n \geq 127 \ . \tag{55}$$

However, if the first-order Reed-Muller code of length 128 (which Mykkeltveit [20] has shown to have covering radius 56) is normal, a question which is still open, we could replace (55) by $t[n,8] \leq [(n-16)/2]$ for $n \geq 127$, in agreement with the conjecture.

To obtain a general lower bound on $t[n, k]$ we begin with the *sphere bound* [8, (3.2)]. This states that if an $[n,k]\,R$ code exists, then

$$1 + \begin{bmatrix} n \\ 1 \end{bmatrix} + \begin{bmatrix} n \\ 2 \end{bmatrix} + \ldots + \begin{bmatrix} n \\ R \end{bmatrix} \geq 2^{n-k} \ . \tag{56}$$

The asymptotic version of this usually found in the literature is for codes of rate greater than zero—see (76) below. For rate zero, (56) leads to the following result, which we have not seen mentioned in the literature.

Theorem 25. *If* $k \to \infty$, $n \to \infty$, *with* $k = o(n^{1/3})$, *then*

$$t[n, k] \geq \frac{1}{2}\, n - \frac{1}{2}\, \theta_k \sqrt{n}\,(1 + o(1)) \ , \tag{57}$$

where θ_k *is defined by* $\Phi(-\theta_k) = 2^{-k}$ *and*

$$\Phi(y) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{y} e^{-x^2/2}\, dx \ . \tag{58}$$

For large k,

$$\theta_k \sim \sqrt{2k \log_e 2} \ . \tag{59}$$

Proof. From (56) and the central limit theorem [10, p. 172]. We omit the details. (59) is from [10, p. 166, Lemma 2].

Asymptotically (57) is quite weak, and can be strengthened to give:

Theorem 26. *For k fixed and* $n \to \infty$,

$$t[n, k] \geq \frac{n - \theta_k 2^{k/2}(1+o(1))}{2} \ . \tag{60}$$

Proof. This follows from the argument used for the lower bound of Theorem 22. We apply (57) with $n = 2^k$ to get a lower bound on $t[2^k, k]$. Then for $n \geq 2^k$ every code must contain a repeated coordinate, and so $t[2^k + 2i, k] \geq t[2^k, k] + i$. (60) follows immediately.

For fixed k, the bounds of Theorems 24 and 26 at least have the same rate of growth, namely $\frac{1}{2}\, n - \text{constant} \cdot 2^{k/2}$. (This solves open problem (10.9) of [8].) Other asymptotic results will be found in Section V.

IV. Saving More Than One Coordinate Over the Direct Sum

The amalgamated direct sum of two codes saves one coordinate over their direct sum. When combining Hamming codes it is sometimes possible to do better. We first show how to save two coordinates.

We shall combine two Hamming codes with parameters $[n_1 = 2^{m_1} - 1\ ,\ k_1 = n_1 - m_1]\ R = 1$ and $[n_2 = 2^{m_2} - 1\ ,\ k_2 = n_2 - m_2]\ R = 1$ to obtain an

$$[n_1 + n_2 - 2\ ,\ k_1 + k_2 - 2]\ R = 2 \tag{61}$$

code. A parity check matrix for the new code is shown in Figure 2. Let $\wedge_i$ denote the set of all binary m_i-tuples except **0** and **1** ($i = 1,2$). Then in Figure 2, $!_1 \subseteq \wedge_1$, $!_2 \subseteq \wedge_2$ are subsets to be specified, and $!_1^c = \wedge_1 \setminus !_1$, $!_2^c = \wedge_1 \setminus !_2$ are the remaining vectors. As usual a bar denotes the binary complement.

Lemma 27. *If* $!_1$ *and* $!_2$ *satisfy*

$$(!_i + !_i) \cup (!_i^c + !_i^c) \supset !_i^c \quad (i = 1,2) , \tag{62}$$

$$!_i + !_i^c \supset !_i \quad (i = 1,2) , \tag{63}$$

$$\overline{!}_1 = !_1 , \tag{64}$$

$$\mathbf{1} \in !_2 + !_2^c , \tag{65}$$

then the code with parity check matrix shown in Figure 2 has covering radius 2.

Proof. The covering radius is 2 if every column vector of length $m_1 + m_2$ can be written as a sum of at most two columns of the parity check matrix. A column $\binom{u}{\mathbf{0}}$, $u \in \wedge_1$, is obtained as $\binom{a}{\mathbf{0}}$, $a \in !_1$, as $\binom{a_1}{\mathbf{0}} + \binom{a_2}{\mathbf{0}}$, $a_1 , a_2 \in !_1$, or as $\binom{a_3}{\mathbf{1}} + \binom{a_4}{\mathbf{1}}$, $a_3 , a_4 \in !_1^c$, using (62). A column $\binom{u}{v}$, $u \in \wedge_1$, $v \in \wedge_2$, is obtained because

$$\frac{!_1}{!_2} \cup \frac{\overline{!}_1}{!_2^c} \cup \frac{!_1^c}{\overline{!}_2} \cup \frac{\overline{!_1^c}}{\overline{!_2^c}} \supseteq \frac{\wedge_1}{\wedge_2} ,$$

an identity which follows directly from (64). The remaining cases are easily checked.

Here is a specific choice for $!_1$ and $!_2$ that satisfies the hypotheses of Lemma 27.

Theorem 28. *Provided* $m_1 \geq 3$ *and* $m_2 \geq 4$, *setting* $!_1^c = \{(10...0)^{tr}, (011...1)^{tr}\}$, $!_2^c = \{(10...0)^{tr} , (011...1)^{tr} , (00...01)^{tr}\}$ *in Figure* 2, *we obtain a code with parameters*

$$[n_1 + n_2 - 2 \ , \ n_1 + n_2 - m_1 - m_2 - 2] \ R = 2 , \tag{66}$$

where $n_1 = 2^{m_1} - 1$, $n_2 = 2^{m_2} - 1$. *Furthermore this code is normal, the coordinate corresponding to the column* $(10...0, \ 11...1)^{tr}$ *being acceptable.*

The smallest example is the [20,13] 2 normal code defined by the parity check matrix

(67). The fifth coordinate is acceptable.

$$\begin{array}{|c|c|c|c|}
\hline
0\,0\,1\,1 & 1\,0 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & 1\,1\,1 \\
0\,1\,0\,1 & 0\,1 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & 1\,1\,1 \\
1\,0\,1\,0 & 0\,1 & 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 & 1\,1\,1 \\
\hline
0\,0\,0\,0 & 1\,1 & 0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1 & 1\,0\,0 \\
0\,0\,0\,0 & 1\,1 & 0\,0\,1\,1\,1\,0\,0\,0\,1\,1\,1 & 0\,1\,0 \\
0\,0\,0\,0 & 1\,1 & 1\,1\,0\,0\,1\,0\,1\,1\,0\,0\,1 & 0\,1\,0 \\
0\,0\,0\,0 & 1\,1 & 0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0 & 0\,1\,1 \\
\hline
\end{array} \tag{67}$$

Proof. This choice for $!_1$ and $!_2$ satisfies (62)-(65), so $R = 2$. It is tedious, although straightforward, to verify that the norm is 5, using Theorem 2, and we leave this to the reader.

Saving more than two coordinates. As the length increases it appears possible to save a much larger number of coordinates. Since these codes mostly lie beyond the range of our table we shall just sketch the method, and give one example. We plan to treat this construction in more detail in a later paper.

The construction. This produces a code with $2m$ parity checks, length $n = 2^{m+1} - 2^a - 1$, and covering radius 2. The parity check matrix is shown in Figure 3. We first choose a code A of length m and dimension a, and let B be a code of dimension $m-a$ such that every m-tuple x can be written uniquely as $x = u+v$, $u \in A$, $v \in B$. We also pick an arbitrary map $\alpha : B \to A$, and a map $\beta : \mathbf{F}_2^m \to A$ that satisfies the following condition.

> For any $u, u' \in A$, $v' \in B$, there must exist $u_1, u_2 \in A$ and $v_1, v_2 \in B$ such that $u_1 + u_2 = u'$, $v_1 + v_2 = v'$, and $\beta(u_1+v_1) + \beta(u_2+v_2) = u$.

(68)

In Figure 3, $M = 2^{m-a} - 1$, and $b_1, \ldots, b_M$ are all the nonzero codewords of B; $N = 2^m - 1$, and $u_1, \ldots, u_N$ are all the nonzero m-tuples.

Lemma 29. *Provided condition* (68) *is satisfied, Figure* 3 *is a parity check matrix for a code with parameters* $[n = 2^{m+1} - 2^a - 1,\ k = n - 2m]$ $R = 2$.

Proof. Again we must show that every $2m$-tuple is a sum of at most two columns of the matrix. The sum of a column on the left,

$$(u_1 + v_1\ ,\ \alpha(v_1))^{tr}\ ,\ \ u_1 \in A\ ,\ v_1 \in B\ ,$$

and a column on the right,

$$(\beta(u_2 + v_2)\ ,\ u_2 + v_2)^{tr}\ ,\ \ u_2 \in A\ ,\ v_2 \in B\ ,$$

is

$$(u_1 + v_1 + \beta(u_2 + v_2)\ ,\ u_2 + v_2 + \alpha(v_1))^{tr}\ , \tag{69}$$

which matches an arbitrary column

$$(u + v\ ,\ u' + v')^{tr}\ ,\ \ u\ ,\ u' \in A\ ,\ \ v\ ,\ v' \in B\ ,$$

unless v happens to be zero. The vectors with $v = 0$ are then matched by the sums

$$(\beta(u_1 + v_1)\ +\ \beta(u_2 + v_2)\ ,\ u_1 + v_1 + u_2 + v_2)^{tr}$$

of two columns on the right, using (68). This completes the proof.

Notice that (69) matches most of the columns, and (68) is not an onerous condition.

For example, define codes A, B by the generator matrices

$$A : \begin{bmatrix} 1\,0\,0\,\ldots\,0 \\ 0\,1\,0\,\ldots\,0 \end{bmatrix},$$

$$B : \begin{bmatrix} 0\,0\,1\,0\,\ldots\,0 \\ 0\,0\,0\,1\,\ldots\,0 \\ \ldots\ldots\ldots \\ 0\,0\,0\,0\,\ldots\,1 \end{bmatrix},$$

and let $\alpha(b)$ select a vector of A according to the third and fourth coordinates of b. Let ζ be a primitive element of $GF(2^m)$, and define β by

$$\beta^{-1}(00\ldots0) = \{\zeta^i : 0 \le i \le 2^m - 2,\ \ i \equiv 3 \pmod 4\},$$

$$\beta^{-1}(10\ldots0) = \{\zeta^i : i \equiv 0 \pmod 4\},$$

$$\beta^{-1}(01\ldots0) = \{\zeta^i : i \equiv 1 \pmod 4\},$$

$$\beta^{-1}(11\ldots0) = \{\zeta^i : i \equiv 2 \pmod 4\}.$$

Although we do not have a general proof, it appears that this choice of β satisfies (68) for all $m \ge 5$. When $m = 5$, for instance, with ζ a primitive element of $GF(32)$ satisfying $\zeta^5 + \zeta^2 + 1 = 0$ (see for example [18, p. 110]), this produces a [59,49] 2 code with the parity check matrix given in Figure 4.

Optimal codes with covering radius 2.

The codes with covering radius 2 constructed in this paper are not too far from optimal. For length $n \le 64$ this can be seen in the main table: in any particular column there is at most one entry ''$t[n, k] = 2$ or 3,'' where although a code of covering radius 2 seems possible, the best code known has covering radius 3. For arbitrary n we have the following result.(2)

Theorem 30. *Let $k^*(n)$ be the smallest value of k such that there exists an $[n, k]$ 2 code. Then for $n \ge 28$,*

(i) *if* $2^{m+1}-4 \le n < 3\cdot 2^m-4$,

$$k^*(n) = n-2m\ ,\quad n-2m-1 \quad or \quad n-2m-2\ ; \tag{70}$$

(ii) *if* $3\cdot 2^m-4 \le n < 2^{m+2}-4$,

$$k^*(n) = n-2m-1 \quad or \quad n-2m-2\ . \tag{71}$$

Remark. A typical column in the table (after transposing) looks like this:

(i) If $2^{m+1}-4 \le n < 3\cdot 2^m-4$, and μ is defined by $2^\mu-1 \le n < 2^{\mu+1}-1$. (The starred entries may be absent, and there are at most two of them.)

k :	n	$n-1$	...	$n-\mu$	$n-\mu-1$	...	$n-2m$	$n-2m-1^*$	$n-2m-2^*$	...
$t[n,k]$:	0	1	...	1	2	...	2	2-3	2-3	3

(ii) If $3\cdot 2^m-4 \le n < 2^{m+2}-4$, and μ is defined by $2^\mu-1 \le n < 2^{\mu+1}-1$. (There is at most one starred entry.)

k :	n	$n-1$	...	$n-\mu$	$n-\mu-1$	...	$n-2m-1$	$n-2m^*$	...
$t[n,k]$:	0	1	...	1	2	...	2	2-3	3

The entries $0,1,...,1,2$ follow from the sphere bound (56) and Hamming codes. The entries at the right-hand end, asserting that codes of covering radius 3 exist, are easily established by combining three Hamming codes. The difficult part is to determine when 2 changes to 2-3 or 3.

Proof. Let k_3 be the real solution of

$$1 + \binom{n}{1} + \binom{n}{2} = 2^{n-k_3}\ ,$$

i.e.

$$k_3 = n+1-\log_2(n^2+n+2) \ . \tag{72}$$

Then if $k < k_3$, $t[n, k] \geq 3$. (i) For $2^{m+1}-4 \leq n < 3 \cdot 2^m - 4$ ($m \geq 4$), we combine two Hamming codes of length $2^m - 1$ as in Theorem 28, to obtain a code of dimension $k_2 = n-2m$ and covering radius 2. The difference,

$$k_2 - k_3 = \log_2(n^2+n+2) - 2m - 1 \ ,$$

is less than 3 for n in this range. Therefore there are at most two entries ''$t[n, k] = 2$ or 3'' in this case. (ii) For $3 \cdot 2^m - 4 \leq n < 2^{m+2} - 4$ ($m \geq 4$), we combine Hamming codes of lengths $2^{m+1} - 1$ and $2^m - 1$ to obtain a code of dimension $k_2 = n - 2m - 1$ and covering radius 2. Then $k_2 - k_3 < 2$, so there is at most one ambiguous entry in this case.

V. The Extended Direct Sum Construction

Theorem 20 produces codes of fixed dimension, i.e. with rate $\rightarrow 0$ as $n \rightarrow \infty$. In this section we present a construction which produces good covering codes of arbitrary length and any desired rate. Although we cannot determine the covering radius of these codes exactly, it is possible to give an upper bound which appears to be fairly close to the true value. We also compare the covering radii of these codes with the optimal value as given by the (nonconstructive) result (76). At the end of the section we briefly describe some related constructions.

Let L (the little code) be an $[n_L, k_L]$ R_L code, and B (the big code) an $[n_L, k_B]$ R_B code of the same length. Their *extended direct sum* is shown in Figure 5(a), and consists

of the direct sum of m copies of L, extended (or augmented) by all vectors formed by repeating any codeword of B m times, where $m = 1,2,3,\ldots$. We use $\mathcal{E}(L, B)$ to denote any of these codes.

Theorem 31. *The extended direct sum* $\mathcal{E}(L, B)$ *has length* $n = mn_L$, *dimension* $k \le mk_L + k_B$, *and covering radius* $R \le [m\Psi(L, B)]$, *where*

$$\Psi(L, B) = \max_{u \in \mathbf{F}_2^{n_L}} \frac{1}{2^{k_B}} \sum_{b \in B} \mathrm{dist}(L, b+u) \ . \tag{73}$$

If $L \subseteq B$, $\mathcal{E}(L, B)$ *has dimension* $mk_L + (k_B - k_L)$—*see Figure* 5(*b*).

Proof. Let $U = (u^{(1)},\ldots,u^{(m)})$, $u^{(i)} \in \mathbf{F}_2^{n_L}$, be an arbitrary vector of length n. For any fixed $b \in B$ we can add codewords of L to U and reduce its weight to

$$\le \sum_{i=1}^{m} \mathrm{dist}(L, b+u^{(i)}) \ .$$

Therefore the covering radius of the new code is

$$\le \max_U \min_{b \in B} \sum_{i=1}^{m} \mathrm{dist}(L, b+u^{(i)})$$

$$\le \max_U \frac{1}{2^{k_B}} \sum_{b \in B} \sum_{i=1}^{m} \mathrm{dist}(L, b+u^{(i)})$$

$$= m\Psi(L, B) \ .$$

Remarks. (i) As we shall see, this construction is yet another illustration of our theme that direct sums can usually be improved. The construction was found by trying to adapt a construction of Davenport's for quadratic forms [9] so as to apply to codes.

(ii) $\Psi(L, B)$ is quite easy to evaluate explicitly. In any case it only needs to be

calculated once, and then applies to all the codes $\mathcal{C}(L, B)$. In evaluating $\Psi(L, B)$, it is enough to consider vectors u which are coset representatives of B. We shall use the notation

$$\Psi_u(L, B) = \frac{1}{2^{k_B}} \sum_{b \in B} \mathrm{dist}(L, b+u) ,$$

so that $\Psi(L, B) = \max_u \Psi_u(L, B)$.

(iii) Two special cases are of particular interest. First, if $L = \{\mathbf{0}, \mathbf{1}\}$, $\Psi_u(L, B)$ can be written down if the weight distributions of the cosets of B are known. Suppose the coset $B+u$ contains $A_i(u)$ vectors of weight i, for $i = 0, 1, \ldots, n_L$. Then

$$\Psi_u(L, B) = \sum_{i=0}^{n_L} A_i(u) \min\{i, n-i\} . \tag{74}$$

Second, if $B = \mathbf{F}_2^{n_L}$, then $u = \mathbf{0}$ is the only possibility, and

$$\Psi(L, B) = \frac{1}{2^{n_L - k_L}} \sum_{i=0}^{R_L} i a_i , \tag{75}$$

where R_L is the covering radius of L and a_i is the number of coset leaders of L of weight i.

(iv) As m increases, the rate of $\mathcal{C}(L, B)$ approaches k_L/n_L, the rate of L.

To test how good these codes are, we will compare them with the (non-constructive) asymptotic result that

$$\frac{1}{n} t[n, \lambda n] \sim H_2^{-1}(1-\lambda) , \quad \text{as} \quad n \to \infty , \tag{76}$$

for a fixed rate λ, $0 < \lambda < 1$, where H_2 is the binary entropy function. (76) appears to

be originally due to Goblick [5, p. 200], although it has been rediscovered several times [7], [30].

Examples of extended direct sums.

A very large number of codes can be obtained from this construction, but we shall just give a few representative examples.

(a) $L = \{0^7, 1^7\}$, B = [7,4] 1 Hamming code. There are only two choices for u, say $u_0 = 00...0$ and $u_1 = 10...0$. The corresponding cosets of B have weight distributions given by:

i	0	1	2	3	4	5	6	7
$A_i(u_0)$	1	0	0	7	7	0	0	1
$A_i(u_1)$	0	1	3	4	4	3	1	0

From (74),

$$\Psi_{u_0}(L, B) = \frac{21}{8}, \quad \Psi_{u_1}(L, B) = \frac{19}{8},$$

and

$$\Psi(L, B) = \max\left\{\frac{21}{8}, \frac{19}{8}\right\} = \frac{21}{8}.$$

From Theorem 31, the codes $\mathcal{C}(L, B)$ have parameters $n = 7m$, $k = m + 3$ and

$$R \leq \left\lceil \frac{21m}{8} \right\rceil. \tag{77}$$

The [21,6] code corresponding to $m = 3$ has generator matrix (78).

1 1 1 1 1 1 1 0 0 0 0 0 0 0	0 0 0 0 0 0 0 1 1 1 1 1 1 1	0 0 0 0 0 0 0 0 0 0 0 0 0 0
1 1 0 1 0 0 0 0 1 1 0 1 0 0 0 0 1 1 0 1 0 0 0 0 1 1 0 1	1 1 0 1 0 0 0 0 1 1 0 1 0 0 0 0 1 1 0 1 0 0 0 0 1 1 0 1	1 1 0 1 0 0 0 0 1 1 0 1 0 0 0 0 1 1 0 1 0 0 0 0 1 1 0 1

(78)

The true covering radius of this code is 6, although (77) only gives $R \le 7$. The parameters of the first few codes in this family are given in the following table, together with the present upper bound on $t[n, k]$.

m	*n*	*k*	(77)	*true R*	*record*
1	7	4	2	1	1
2	14	5	5	4	4
3	21	6	7	6	6
4	28	7	10	9	9
5	35	8	13	12 or 13	12
6	42	9	15	?	15
7	49	10	18	?	18
8	56	11	21	?	20
9	63	12	23	?	23

(79)

These are quite respectable codes. For large n, these codes have rate approaching 1/7, and the upper bound on R/n approaches $3/8 = 0.375$. On the other hand the direct sum of m copies of L also has rate 1/7, while $R/n = 3/7 = 0.429...$.

(b) $L = \{0, 1\}$, $B = \mathbf{F}_2$. In this case the codewords of $\mathcal{C}(L, B)$ are best written in an $n \times m$ rectangle, and the generators are all single rows and single columns:

$$\begin{bmatrix} & & \\ 1 & 1 & 1 \ . \ . \ . \ 1 \\ & & \end{bmatrix}, \quad \begin{bmatrix} 1 \\ 1 \\ . \ . \ . \\ 1 \end{bmatrix}$$

The parameters are $[n = , m, k = , + m - 1]$, and covering radius $R = g(, , m)$ say.

This code arises in the Berlekamp-Gale switching problem. Consider an $, \times m$ array of lightbulbs, controlled by $, + m$ switches, one for each row and column. When a switch is thrown, all lights in the corresponding row or column that are off turn on, and those that are on turn off. For each initial pattern S of lights, let $f(S)$ be the minimal number of lights that are on after throwing the switches in any way. The problem is to determine $\max_S f(S)$, which is precisely $g(, , m)$. This has been studied by several authors (see [4], [6], [12]). For example $g(, , m)$ is known exactly for $, \leq 4$ [6].

In evaluating (74) only $u = \mathbf{0}$ need be considered, and after some simplification we find

$$\Psi(L, B) = \frac{1}{2}\, , \; - \frac{,}{2'} \left\lceil \frac{, -1}{\tfrac{1}{2}(, -1)} \right\rceil$$

when $,$ is odd, which is the most interesting case. Therefore the covering radius of these codes, $g(, , m)$, does not exceed

$$\frac{, m}{2} - , m \cdot \min \left\{ \frac{1}{2'} \left\lceil \frac{, -1}{\tfrac{1}{2}(, -1)} \right\rceil , \quad \frac{1}{2^m} \left\lceil \frac{m-1}{\tfrac{1}{2}(m-1)} \right\rceil \right\} , \tag{80}$$

if $,$ and m are both odd. This bound could also be obtained from Theorem 3 of [12]. For $, = 7$ we have $[n = 7m, \; k = m+6]$, $R \leq [77m/32]$, giving the following codes:

m	n	k	$R \leq$	*true* R	*record*
1	7	7	2	1	1
2	14	8	4	3	2
3	21	9	7	5	5
4	28	10	9	8	7
5	35	11	12	?	9
6	42	12	14	?	12
7	49	13	16	?	15
8	56	14	19	?	18
9	63	15	21	?	21

(81)

Again these are quite good. For large n, their rate approaches 1/7, and $R/n \leq 0.344...$.

On the other hand, from (76), we know there exist codes of rate 1/7 and $R/n \sim H_2^{-1}(6/7) = 0.281...$. In summary, for rate 1/7, we have these values of R/n:

direct sum construction	0.429...
example (a)	0.375...
example (b)	0.344...
existence result (76)	0.281...

When the parameter , itself is large, the codes of example (b) have rate approaching $1/$, as $n \to \infty$ and, from (80),

$$\frac{R}{n} \leq \frac{1}{2} - \frac{1}{\sqrt{2\pi,}} + ... = \frac{1}{2} - \frac{0.399...}{\sqrt{,}} + ... \tag{82}$$

For comparison, the direct sum of m copies of L has the same rate and $R/n \to 0.5$, while from (76) we know that there exist codes of this rate with

$$\frac{R}{n} \sim H_2^{-1}\left(1 - \frac{1}{,}\right) = \frac{1}{2} - \sqrt{\frac{\log_e 2}{2,}} + ...$$

$$= \frac{1}{2} - \frac{0.589}{\sqrt{,}} + ... \tag{83}$$

(c) $L = [7,4]$ 1 Hamming code, $B = \mathbf{F}_2^7$. Now $\mathcal{C}(L, B)$ has $n = 7m$, $k = 4m+3$, and rate $\to 4/7$ as $m \to \infty$. B has one coset leader of weight 0 and seven of weight 1, so $\Psi(L, B) = 7/8$ from (75), and the codes have covering radius $R \le [7m/8]$, and $R/n \le 0.125$. For comparison the direct sum of Hamming codes has the same rate and $R/n = 0.143...$, while from (76) we know that there exist codes with $R/n \sim H_2^{-1}(3/7) = 0.088...$.

Bordered extended direct sums.

Two of the optimal codes given in Section III, the [15,6] 3 code (46) and the [19,6] 5 code (47), have the form of an extended direct sum with a *border* of a small number of further coordinates added on the left. Generalizing (46), for example, we obtain $[n = 3m+2,\ k = m+2]$ codes with the generators matrices shown in (84).

$$\begin{array}{|c|c|c|c|c|}
\hline
1\,1 & 1\,1\,1 & 0\,0\,0 & \ldots & 0\,0\,0 \\
1\,1 & 0\,0\,0 & 1\,1\,1 & \ldots & 0\,0\,0 \\
 & \ldots & & \ldots & \\
1\,1 & 0\,0\,0 & 0\,0\,0 & \ldots & 1\,1\,1 \\
\hline
1\,0 & 1\,0\,0 & 1\,0\,0 & \ldots & 1\,0\,0 \\
0\,1 & 0\,1\,0 & 0\,1\,0 & \ldots & 0\,1\,0 \\
\hline
\end{array} \tag{84}$$

The first few codes of this type are as follows.

m	n	k	R	*record*
1	5	3	2	1
2	8	4	2	2
3	11	5	3	3
4	14	6	3	3
5	17	7	4	4
6	20	8	5	5
7	23	9	6	6
8	26	10	6	6
9	29	11	7	7
10	32	12	≥ 8	7

(85)

VI. The Main Table; Other Constructions; Open Problems

We now collect the results of all the previous sections and assemble a table of $t[n, k]$ for $n \le 64$. An entry such as $t[32,10] = 7\text{-}9$ indicates that $7 \le t[32,10] \le 9$. The rows $k = 1$ to 5 are special in that the exact value of $t[n, k]$ is known for all n from (40)-(42) and Theorems 21, 22. For $k \ge 6$, the lower bound is given by the sphere bound (56), with the single exception, noted just below Theorem 23, of $t[12,6]$. For $k \ge 6$ the upper bounds, which are all obtained by explicit construction, were found as follows. The unmarked entries are obtained *either* from an adjacent entry via one of the rules

$$t[n, k] \le t[n-1, k-1] \ , \tag{86}$$

$$t[n, k] \le t[n, k-1] \ , \tag{87}$$

$$t[n, k] \le t[n+1, k] \tag{88}$$

(see (37)-(39)), *or* from the entry two squares to the left, via

$$t[n, k] \le t[n-2, k] + 1 \ , \tag{89}$$

using Theorem 20. The latter is justified because we were careful to check that every code entered into the table was normal (with perhaps the single exception of the [59,49] 2 code of Figure 4).

The marked entries in the table correspond to exceptionally good covering codes. We have only marked codes that could not be obtained by one of the rules (86)-(89). Thus

although many cyclic codes, for example, are equal to the present record value for $t[n, k]$ (see below), they are not mentioned in the table because codes with the same parameters can already be obtained more simply from (86)-(89).

The marked entries are of five types.

a: An amalgamated direct sum of normal codes, obtained via the formula

$$[n_1+n_2-1, k_1+k_2-1]\ R_1+R_2 = [n_1, k_1]\ R_1 \dot{\oplus} [n_2, k_2]\ R_2\ . \qquad (90)$$

See the examples (34)-(36).

b: By saving two coordinates over a direct sum (see (61)).

The remaining three types are the true ‘‘seeds,’’ the codes from which all the others are derived.

g: Golay or shortened Golay code.

h: Hamming code.

s: The following special seeds.

n	*k*	*R*	*remarks*
14	6	3	(46).
19	6	5	(47).
31	11	7	BCH code, $d_{\min} = 11$.
59	49	2	Figure 4.

Other constructions We mention here some other constructions that were not so successful in producing new records. However, as mentioned in the introduction, it is often useful to have alternative ways of finding codes with given parameters.

(a) Cyclic codes. We determined the covering radius of most cyclic codes of length ≤ 35, but only found one new record, the [31,11] 7 BCH code. On the other hand, in a number of cases cyclic codes were as good as any codes known. For example, at length 21, let the factors of $x^{21}+1$ be labeled as follows:

$$x^{21}+1 = (x+1)(x^2+x+1)(x^3+x+1)(x^3+x^2+1) \cdot$$
$$\cdot (x^6+x^4+x^2+x+1)(x^6+x^5+x^4+x^2+1)$$
$$= \phi_1\ \phi_2\ \phi_3\ \psi_3\ \phi_6\ \psi_6 \quad \text{(say)} .$$

Then the next table shows that cyclic codes are as good as any, for all dimensions $5 \leq k \leq 13$ except $k = 8$. $g(x)$ denotes the generator polynomial.

n	k	R	$g(x)$	*record*
21	5	8	$\phi_1\ \phi_3\ \phi_6\ \psi_6$	8
21	6	6	$\phi_3\ \phi_6\ \psi_6$	6
21	7	6	$\phi_2\ \phi_3\ \psi_3\ \phi_6$	6
21	9	5	$\phi_6\ \psi_6$	5
21	10	4	$\phi_2\ \phi_3\ \phi_6$	4
21	11	4	$\phi_1\ \phi_3\ \phi_6$	4
21	12	3	$\phi_3\ \phi_6$	3
21	13	3	$\phi_2\ \phi_6$	3

(91)

(b) The ‘‘double overlap’’ construction. It is natural to try to generalize the a.d.s. construction of Figure 1(d) by overlapping two coordinates, as illustrated in Figure 6. This shows a [12,6] 3 code formed by overlapping two [7,4] 1 Hamming codes. Three Hamming codes combine in the same way to produce a [17,8] 4 code. We have analyzed these codes by extending the notion of norm in the appropriate way, but in general the results are not impressive and we shall not describe the theory here.

(c) Other published codes. As the bibliography in [18] shows, a very large number

of error-correcting codes have been published in the last 35 years. We calculated the covering radius of many of these codes, but the results were disappointing, as no new records were found. Even the codes found by Fontaine and Peterson [11] and Tokura, Taniguchi and Kasami [27], which have the lowest possible error probability, and therefore a small number of cosets of high weight, did not improve on the codes constructed in this paper. The following are some typical examples of codes we found in the literature that have covering radius equal to the present record for $t[n, k]$.

n	k	R	$d_{\min}$	*source*
13	7	2	3	[11]
14	7	3	4	[26]
19	10	3	5	[29]
22	12	3	5	[11]
23	7	7	9	[14]
26	9	7	9	[13]
27	10	7	9	[24]
30	12	7	9	[13]

(92)

The code of length 19 in (92) is a quasi-perfect double-error-correcting code, which therefore has covering radius 3. References [23] and [27]-[29] contain many other examples of such codes. It is worth mentioning that some of our new codes fill certain gaps in the old tables of quasi-perfect codes. For example our [13,7] $R = 2$, $d_{\min} = 3$ and [19,12] $R = 2$, $d_{\min} = 3$ codes could be added to the table of quasi-perfect codes in Peterson and Weldon [23, page 122].

Open problems.

(i) Find an example of a code that is not normal (see Section II).

(ii) Lemma 16 and Corollaries 17, 18 seem quite weak, and in particular it should be possible to strengthen the upper bound in (32).

(iii) Settle the conjectures (50), (51). A significant step in this direction would be to determine whether all first-order Reed-Muller codes are normal (see Theorem 14). The first open case is the [128,8] 56 code (see the remark following Theorem 24).

(iv) Settle the early gaps in the main table: is $t[15,6] = 3$ or 4, $t[17,6] = 4$ or 5, $t[16,10] = 2$ or 3, etc.? There are quite large gaps towards the end of the table, and it seem likely that cyclic codes of length 63, for example, should improve on some of these entries.

(v) Determine the true covering radius of the codes in (79), (81), etc.

(vi) Finally, in (73) the maximum of $\Psi(L, B)$ is often attained when $u = \mathbf{0}$. For which codes is this true?

Acknowledgements

We are grateful to Gérard Cohen, Mark Karpovsky, Skip Mattson and Jim Schatz for allowing us to see a preprint of [8]. We also acknowledge helpful conversations with Toby Berger, Fan Chung, Gérard Cohen, John Conway, Colin Mallows and Andrew Odlyzko, and we thank Jeff Leon for allowing us to use his code automorphism program [17]. Finally we thank the referees for some very helpful comments.

List of footnotes

(1) I.e. a subcode C_0 such that $C = C_0 \cup (a + C_0)$ where $a \notin C_0$.

(2) A similar but slightly weaker result has been obtained by Gérard Cohen (personal communication).

List of Table Captions

Table of $t[n, k]$. Section 1.

Table of $t[n, k]$. Section 2.

Table of $t[n, k]$. Section 3.

Table of $t[n, k]$. Section 4.

Table of $t[n, k]$. Section 5.

Table of $t[n, k]$. Section 6.

Table of $t[n, k]$. Section 7.

Table of $t[n, k]$. Section 8.

Table of $t[n, k]$. Section 9.

Table of $t[n, k]$. Section 10.

Table of $t[n, k]$. Section 11.

Table of $t[n, k]$. Section 12.

TABLE OF $t[n, k]$. SECTION 1

K	N=	1	2	3	4	5	6	7	8	9	10	11
1		0	1	1	2	2	3	3	4	4	5	5
2			0	1	1	2	2	3	3	4	4	5
3				0	1	1	2	2	3	3	4	4
4					0	1	1	1^h	2	2	3	3
5						0	1	1	1	2	2	3
6							0	1	1	1	2	2
7								0	1	1	1	2
8									0	1	1	1
9										0	1	1
10											0	1
11												0

TABLE OF $t[n, k]$. SECTION 2

K	N=	12	13	14	15	16	17	18	19	20	21	22
1		6	6	7	7	8	8	9	9	10	10	11
2		5	6	6	7	7	8	8	9	9	10	10
3		5	5	6	6	7	7	8	8	9	9	10
4		4	4	5	5	6	6	7	7	8	8	9
5		3	4	4	5	5	6	6	7	7	8	8
6		3	3	3^s	3-4	4	4-5	5	5^s	5-6	6	6-7
7		2	2^a	3	3	3-4	4	4-5	4-5	5	5-6	5-6
8		2	2	2	3	3	3-4	4	4-5	4-5	5	5-6
9		1	2	2	2	2-3	3	3-4	3-4	4^a	4-5	4-5
10		1	1	2	2	2	2-3	3	3^a	3-4	4	4-5
11		1	1	1	1^h	2	2	2-3	3	3	3-4	4
12		0	1	1	1	1	2	2	2^g	3	3	3
13			0	1	1	1	1	2	2	2	3	3
14				0	1	1	1	1	2	2	2	3
15					0	1	1	1	1	2	2	2
16						0	1	1	1	1	2	2
17							0	1	1	1	1	2
18								0	1	1	1	1
19									0	1	1	1
20										0	1	1
21											0	1
22												0

TABLE OF $t[n, k]$. SECTION 3

K	N= 23	24	25	26	27	28	29	30	31	32	33
1	11	12	12	13	13	14	14	15	15	16	16
2	11	11	12	12	13	13	14	14	15	15	16
3	10	11	11	12	12	13	13	14	14	15	15
4	9	10	10	11	11	12	12	13	13	14	14
5	9	9	10	10	11	11	12	12	13	13	14
6	6-7	7-8	7-8	8-9	8-9	8-10	9-10	9-11	10-11	10-12	10-12
7	6-7	6-7	7-8	7-8	7-9	8-9	8-10	8-10	9-11	9-11	10-12
8	5-6	6-7	6-7	6-8	7-8	7-9	7-9	8-10	8-10	9-11	9-11
9	5-6	5-6	5-6[a]	6-7	6-7	7-8	7-8	7-9	8-9	8-10	8-10
10	4-5	5-6	5-6	5-6	6-7	6-7	6-8	7-8	7-9	7-9	8-10
11	4-5	4-5	5-6	5-6	5-6	6-7	6-7	6-7	7[s]	7-8	7-8
12	3[g]	4	4	4-5	5	5-6	5-6	6-7	6-7	6-7	7-8
13	3	3	4	4	4-5	5	5-6	5-6	6-7	6-7	6-7
14	3	3	3	4	4	4-5	5	5-6	5-6	6-7	6-7
15	2-3	3	3	3	4	4	4[a]	5	5	5-6	5-6
16	2	2-3	3	3	3	4	4	4	4-5	5	5-6
17	2	2	2-3	3	3	3	4	4	4	4-5	5
18	2	2	2	2-3	3	3	3	3-4	4	4	4-5
19	1	2	2	2	2-3	3	3	3	3-4	4	4
20	1	1	2	2	2	2[b]	3	3	3	3-4	4
21	1	1	1	2	2	2	2	3	3	3	3-4
22	1	1	1	1	2	2	2	2	3	3	3

TABLE OF $t[n, k]$. SECTION 4

K	N= 23	24	25	26	27	28	29	30	31	32	33
23	0	1	1	1	1	2	2	2	2	2-3	3
24		0	1	1	1	1	2	2	2	2	2-3
25			0	1	1	1	1	2	2	2	2
26				0	1	1	1	1	1[h]	2	2
27					0	1	1	1	1	1	2
28						0	1	1	1	1	1
29							0	1	1	1	1
30								0	1	1	1
31									0	1	1
32										0	1
33											0

TABLE OF $t[n, k]$. SECTION 5

K	N= 34	35	36	37	38	39	40	41	42	43	44
1	17	17	18	18	19	19	20	20	21	21	22
2	16	17	17	18	18	19	19	20	20	21	21
3	16	16	17	17	18	18	19	19	20	20	21
4	15	15	16	16	17	17	18	18	19	19	20
5	14	15	15	16	16	17	17	18	18	19	19
6	11-13	11-13	12-14	12-14	12-15	13-15	13-16	14-16	14-17	14-17	15-18
7	10-12	10-13	11-13	11-14	12-14	12-15	12-15	13-16	13-16	14-17	14-17
8	9-12	10-12	10-13	11-13	11-14	11-14	12-15	12-15	12-16	13-16	13-17
9	9-11	9-11	9-12	10-12	10-13	11-13	11-14	11-14	12-15	12-15	13-16
10	8-10	9-11	9-11	9-12	10-12	10-13	10-13	11-14	11-14	12-15	12-15
11	8-9	8-9	8-10	9-10[a]	9-11	9-11	10-12	10-12	11-13	11-13	11-14
12	7-8	7-9	8-9	8-10	9-10	9-11	9-11	10-12	10-12	10-13	11-13
13	7-8	7-8	7-9	8-9	8-10	8-10	9-11	9-11	9-12	10-12	10-13
14	6-7	7-8	7-8	7-8[a]	8-9	8-9	8-10	9-10	9-11	9-11[a]	10-12
15	6-7	6-7	6-8	7-8	7-8	7-9	8-9	8-10	8-10	9-11	9-11
16	5-6	6-7	6-7	6-8	7-8	7-8	7-9	8-9	8-10	8-10	9-10[a]
17	5-6	5-6	6[a]	6-7	6-7	7-8	7-8	7-8[a]	8-9	8-9	8-10
18	5	5[a]	5-6	6	6-7	6-7	6-8	7-8	7-8	7-9	8-9
19	4-5	5	5	5-6	5-6	6-7	6-7	6-8	7-8	7-8	7-9
20	4	4-5	4-5	5	5-6	5-6	6-7	6-7	6-7[a]	7-8	7-8
21	4	4	4-5	4-5	5	5-6	5-6	6[a]	6-7	6-7	7-8
22	3-4	4	4	4[a]	4-5	5	5-6	5-6	6	6-7	6-7

TABLE OF $t[n, k]$. SECTION 6

K	N=	34	35	36	37	38	39	40	41	42	43	44
23		3	3-4	4	4	4	4-5	5	5^a	5-6	5-6	6
24		3	3	3-4	3-4	4	4	4-5	5	5	5-6	5-6
25		2-3	3	3	3-4	3-4	4	4	4-5	5	5	5-6
26		2	2-3	3	3	3-4	3-4	4	4	4-5	4-5	5
27		2	2	2-3	3	3	3-4	3-4	4	4	4-5	4-5
28		2	2	2	2-3	3	3	3-4	3-4	4	4	4-5
29		1	2	2	2	2-3	3	3	3-4	3-4	4	4
30		1	1	2	2	2	2-3	3	3	3^a	3-4	4
31		1	1	1	2	2	2	2-3	3	3	3	3-4
32		1	1	1	1	2	2	2	2-3	3	3	3
33		1	1	1	1	1	2	2	2	2-3	3	3
34		0	1	1	1	1	1	2	2	2	2-3	3
35			0	1	1	1	1	1	2	2	2	2^b
36				0	1	1	1	1	1	2	2	2
37					0	1	1	1	1	1	2	2
38						0	1	1	1	1	1	2
39							0	1	1	1	1	1
40								0	1	1	1	1
41									0	1	1	1
42										0	1	1
43											0	1
44												0

TABLE OF $t[n, k]$. SECTION 7

K	N=	45	46	47	48	49	50	51	52	53	54	55
1		22	23	23	24	24	25	25	26	26	27	27
2		22	22	23	23	24	24	25	25	26	26	27
3		21	22	22	23	23	24	24	25	25	26	26
4		20	21	21	22	22	23	23	24	24	25	25
5		20	20	21	21	22	22	23	23	24	24	25
6		15-18	16-19	16-19	17-20	17-20	17-21	18-21	18-22	19-22	19-23	20-23
7		14-18	15-18	15-19	16-19	16-20	17-20	17-21	17-21	18-22	18-22	19-23
8		14-17	14-18	14-18	15-19	15-19	16-20	16-20	17-21	17-21	17-22	18-22
9		13-16	13-17	14-17	14-18	15-18	15-19	15-19	16-20	16-20	17-21	17-21
10		12-16	13-16	13-17	13-17	14-18	14-18	15-19	15-19	15-20	16-20	16-21
11		12-14	12-15	12-15	13-16	13-16	14-17	14-17	14-18	15-18	15-19	15-19
12		11-14	11-14	12-15	12-15	13-16	13-16	13-17	14-17	14-18	14-18	15-19
13		10-13	11-14	11-14	12-15	12-15	12-16	13-16	13-17	13-17	14-18	14-18
14		10-12	10-13	11-13	11-14	11-14	12-15	12-15	12-16	13-16	13-17	14-17
15		9-12	10-12	10-13	10-13	11-14	11-14	12-15	12-15	12-16	13-16	13-17
16		9-11	9-11	10-12	10-12	10-12[a]	11-13	11-13	11-14	12-14	12-15	12-15[a]
17		8-10	9-11	9-11	10-12	10-12	10-12	11-13	11-13	11-14	12-14	12-15
18		8-10	8-10	9-11	9-11	9-12	10-12	10-12	10-13	11-13	11-14	11-14
19		8-9	8-10	8-10	9-11	9-11	9-11[a]	10-12	10-12	10-13	11-13	11-13[a]
20		7-9	8-9	8-9[a]	8-10	8-10	9-11	9-11	9-12	10-12	10-13	10-13
21		7-8	7-9	7-9	8-9	8-10	8-10	9-11	9-11	9-12	10-12	10-13
22		6-8	7-8	7-9	7-9	8-9	8-10	8-10	9-10	9-10[a]	9-11	10-11

TABLE OF $t[n, k]$. SECTION 8

K	N=	45	46	47	48	49	50	51	52	53	54	55
23		6[a]	6-7	7	7-8	7-8	8-9	8-9	8-10	9-10	9-10	9-11
24		6	6	6-7	7	7-8	7-8	7-9	8-9	8-10	8-10	9-10
25		5-6	6	6	6-7	7	7-8	7-8	7-9	8-9	8-10	8-10
26		5-6	5-6	6	6	6-7	6-7	7[a]	7-8	8-9	8-9	
27		5	5-6	5-6	6	6	6-7	6-7	7	7-8	7-8	8-9
28		4-5	5	5-6	5-6	5-6	6	6-7	6-7	7	7-8	7-8
29		4-5	4-5	5	5-6	5-6	5-6	6	6-7	6-7	7	7-8
30		4	4-5	4-5	5	5-6	5-6	5-6	6	6-7	6-7	7
31		4	4	4-5	4-5	5	5[a]	5-6	5-6	6	6-7	6-7
32		3-4	4	4	4-5	4-5	5	5	5-6	5-6	6	6-7
33		3	3-4	3-4	4	4-5	4-5	4-5	5	5-6	5-6	6
34		3	3	3-4	3-4	4	4-5	4-5	4-5	5	5-6	5-6
35		2-3	3	3	3-4	3-4	4	4-5	4-5	4-5	5	5-6
36		2	2-3	3	3	3-4	3-4	4	4-5	4-5	4-5	5
37		2	2	2-3	3	3	3-4	3-4	4	4[a]	4-5	4-5
38		2	2	2	2-3	3	3	3-4	3-4	4	4	4-5
39		2	2	2	2	2-3	3	3	3-4	3-4	4	4
40		1	2	2	2	2	2-3	3	3	3-4	3-4	4
41		1	1	2	2	2	2	2-3	3	3	3-4	3-4
42		1	1	1	2	2	2	2	2-3	3	3	3-4
43		1	1	1	1	2	2	2	2	2-3	3	3
44		1	1	1	1	1	2	2	2	2	2-3	3

TABLE OF $t[n, k]$. SECTION 9

K	N=	45	46	47	48	49	50	51	52	53	54	55
45		0	1	1	1	1	1	2	2	2	2	2-3
46			0	1	1	1	1	1	2	2	2	2
47				0	1	1	1	1	1	2	2	2
48					0	1	1	1	1	1	2	2
49						0	1	1	1	1	1	2
50							0	1	1	1	1	1
51								0	1	1	1	1
52									0	1	1	1
53										0	1	1
54											0	1
55												0

TABLE OF $t[n, k]$. SECTION 10

K	N=	55	56	57	58	59	60	61	62	63	64
1		27	28	28	29	29	30	30	31	31	32
2		27	27	28	28	29	29	30	30	31	31
3		26	27	27	28	28	29	29	30	30	31
4		25	26	26	27	27	28	28	29	29	30
5		25	25	26	26	27	27	28	28	29	29
6		20-23	20-24	20-24	21-25	21-25	22-26	22-26	23-27	23-27	23-28
7		19-23	19-23	19-24	20-24	20-25	21-25	21-26	22-26	22-27	22-27
8		18-22	18-23	19-23	19-24	19-24	20-25	20-25	21-26	21-26	21-27
9		17-21	17-22	18-22	18-23	19-23	19-24	19-24	20-25	20-25	21-26
10		16-21	17-21	17-22	17-22	18-23	18-23	19-24	19-24	19-25	20-25
11		15-19	16-20	16-20	17-21	17-21	17-22	18-22	18-23	19-23	19-24
12		15-19	15-19	16-20	16-20	16-21	17-21	17-22	17-22	18-23	18-23
13		14-18	15-19	15-19	15-20	16-20	16-21	16-21	17-22	17-22	18-23
14		14-17	14-18	14-18	15-19	15-19	15-20	16-20	16-21	17-21	17-22
15		13-17	13-17	14-18	14-18	14-19	15-19	15-20	16-20	16-21	16-21
16		12-15	13-16	13-16	14-17	14-17	14-18	15-18	15-19	15-19	16-20
17		12-15	12-15	13-16	13-16	13-17	14-17	14-18	14-18	15-19	15-19
18		11-14	12-15	12-15	12-16	13-16	13-17	13-17	14-18	14-18	15-19
19		11-13	11-14	12-14	12-15	12-15	13-16	13-16[a]	13-17	14-17	14-18
20		10-13	11-13	11-14	11-14	12-15	12-15	12-16	13-16	13-17	14-17
21		10-13	10-13	11-13	11-14	11-14	12-14	12-14[a]	12-15	13-15	13-16
22		10-11	10-12	10-12	11-13	11-13[a]	11-14	12-14	12-14	12-15	13-15

TABLE OF $t[n, k]$. SECTION 11

K	N=	55	56	57	58	59	60	61	62	63	64
23		9-11	9-11	10-12	10-12	10-13	11-13	11-14	11-14	12-14	12-15
24		9-10	9-11	9-11	10-12	10-12	10-13	11-13	11-14	11-14	12-14
25		8-10	9-10	9-11	9-11	10-11[a]	10-12	10-12	11-13	11-13	11-14
26		8-9	8-10	9-10	9-11	9-11	9-11	10-12	10-12	10-13	11-13
27		8-9	8-9	8-10	8-10	9-11	9-11	9-11	10-12	10-12	10-13
28		7-8	7-9	8-9	8-9[a]	8-10	9-10	9-11	9-11	10-11[a]	10-12
29		7-8	7-8	7-8[a]	8-9	8-10	9-10	9-11	9-11	10-11	
30		7	7-8	7-8	7-8	8-9	8-9	8-10	9-10	9-11	9-11
31		6-7	6-7	7-8	7-8	7-8	8-9	8-9	8-10	8-10	9-10[a]
32		6-7	6-7	6-7	7-8	7-8	7-8	8-9	8-9	8-9[a]	8-10
33		6	6-7	6-7	6-7	7[a]	7-8	7-8	7-9	8-9	8-9
34		5-6	5-6	6-7	6-7	6-7	7	7-8	7-8	7-8[a]	8-9
35		5-6	5-6	5-6	6-7	6-7	6-7	7	7-8	7-8	7-8
36		5	5-6	5-6	5-6	6-7	6-7	6-7	6-7	7-8	7-8
37		4-5	5	5-6	5-6	5-6	6-7	6-7	6-7	6-7	7-8
38		4-5	4-5	5	5-6	5-6	5-6	6-7	6-7	6-7	6-7
39		4	4-5	4-5	5	5-6	5-6	5-6	6-7	6-7	6-7
40		4	4	4-5	4-5	5	5-6	5-6	5-6	6-7	6-7
41		3-4	4	4	4-5	4-5	5	5-6	5-6	5-6	6[a]
42		3-4	3-4	4	4	4-5	4-5	4-5	5-6	5-6	5-6
43		3	3-4	3-4	4	4	4-5	4-5	4-5	5-6	5-6
44		3	3	3-4	3-4	3-4	4	4-5	4-5	4-5	5-6

TABLE OF $t[n, k]$. SECTION 12

K	N=	55	56	57	58	59	60	61	62	63	64
45		2-3	3	3	3^a	3-4	3-4	4	4-5	4-5	4-5
46		2	2-3	3	3	3	3-4	3-4	4	4-5	4-5
47		2	2	2-3	3	3	3	3-4	3-4	4	4-5
48		2	2	2	2-3	3	3	3	3-4	3-4	4
49		2	2	2	2	2^s	3	3	3	3-4	3-4
50		1	2	2	2	2	2	3	3	3	3-4
51		1	1	2	2	2	2	2	3	3	3
52		1	1	1	2	2	2	2	2	3	3
53		1	1	1	1	2	2	2	2	2	2-3
54		1	1	1	1	1	2	2	2	2	2
55		0	1	1	1	1	1	2	2	2	2
56			0	1	1	1	1	1	2	2	2
57				0	1	1	1	1	1	1^h	2
58					0	1	1	1	1	1	1
59						0	1	1	1	1	1
60							0	1	1	1	1
61								0	1	1	1
62									0	1	1
63										0	1
64											0

Figure Captions

Figure 1. The amalgamated direct sum (a.d.s.) construction. Choose generator matrices for codes B, C as shown in (a), (b), where the starred columns are acceptable. Their direct sum is shown in (c) and their a.d.s. in (d). The a.d.s. may also be specified in terms of parity check matrices as in (e).

Figure 2. Parity check matrix for code of length $2^{m_1} + 2^{m_2} - 4$ and covering radius 2.

Figure 3. Parity check matrix for code of length $2^{m+1} - 2^a - 1$ and covering radius 2.

Figure 4. Parity check matrix for [59,49] $R = 2$ code, illustrating the construction in Figure 3.

Figure 5. (a) Extended direct sum $\%(L, B)$ of two codes L and B. (b) $\%(L, B)$ in the case when $L \subseteq B$: the last copy of L can be omitted.

Figure 6. The ‘‘double overlap’’ construction.

References

1. B. S. Atal, *Predictive coding of speech at low bit rates,* IEEE Trans. Communications, **COM-30** (1982), 600-614.

2. B. S. Atal and M. R. Schroeder, *Predictive coding of speech signals and subjective error criteria,* IEEE Trans. Acoustics, Speech, Sig. Proc., **ASSP-27** (1979), 247-254.

3. B. S. Atal and M. R. Schroeder, Personal communication.

4. J. Beck and J. H. Spencer, *Balancing matrices with line shifts,* Combinatorica, **3** (1983), 299-304.

5. T. Berger, *Rate Distortion Theory*, Prentice-Hall, Englewood Cliffs, N.J., 1971.

6. T. A. Brown and J. H. Spencer, *Minimization of* ± 1 *matrices under line shifts,* Colloq. Math., **23** (1971), 165-171.

7. G. D. Cohen, *A nonconstructive upper bound on covering radius,* IEEE Trans. Information Theory, **IT-29** (1983), 352-353.

8. G. D. Cohen, M. R. Karpovsky, H. F. Mattson, Jr., and J. R. Schatz, *Covering radius — survey and recent results,* IEEE Trans. Information Theory, to appear.

9. H. Davenport, *The covering of space by spheres*, Rend. Circ. Mat. Palermo, (2)**5** (1956), 1-16.

10. W. Feller, *An Introduction to Probability Theory and Its Applications*, Vol. 1, 2nd edition, 1957, Wiley, N.Y.

11. A. B. Fontaine and W. W. Peterson, *Group code equivalence and optimum codes,* IRE Trans. Information Theory, **IT-5** (1959), 60-70.

12. Y. Gordon and H. S. Witsenhausen, *On extensions of the Gale-Berlekamp switching problem and constants of* , $_p$ *-spaces,* Israel J. Math., **11** (1972), 216-229.

13. A. A. Hashim and A. G. Constantinides, *Some new results on binary linear block codes,* Electronics Letters, **10** (1974), 31-33.

14. A. A. Hashim and V. S. Pozdniakov, *Computerised search for linear binary codes,* Electronics Letters, **12** (1976), 350-351.

15. H. J. Helgert, *Noncyclic generalizations of BCH and Srivastava codes,* Information and Control, **21** (1972), 280-290.

16. T. Helleseth, T. Kløve and J. Mykkeltveit, *On the covering radius of binary codes,* IEEE Trans. Information Theory, **IT-24** (1978), 627-628.

17. J. S. Leon, *Computing automorphism groups of error correcting codes,* IEEE Trans. Information Theory, **IT-28** (1982), 496-511.

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

19. G. L. Movsisyan, *The covering radius of subsets of points of a unit n-dimensional cube* (in Russian), Akad. Nauk Armyan SSR Dokl., **75** (1982, issue 2), 55-59. [Math. Reviews 84i: 94046.]

20. J. Mykkeltveit, *The covering radius of the* (128,8) *Reed-Muller code is 56,* IEEE Trans. Information Theory, **IT-26** (1980), 359-362.

21. A. Nijenhaus and H. S. Wilf, *Combinatorial Algorithms*, Academic Press, N.Y., 2nd edition, 1978.

22. N. J. Patterson and D. H. Wiedemann, *The covering radius of the* $(2^{15}, 16)$ *Reed-Muller code is at least 16276*, IEEE Trans. Information Theory, **IT-29** (1983), 354-356.

23. W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes*, MIT Press, Cambridge, Mass., 2nd edition, 1972.

24. P. Piret, *Good linear codes of length 27 and 28*, IEEE Trans. Information Theory, **IT-26** (1980), 227.

25. O. S. Rothaus, *On ''bent'' functions*, J. Combinatorial Theory, **20A** (1976), 300-305.

26. H. C. A. van Tilborg, *On quasi-cyclic codes with rate* $1/m$, IEEE Trans. Information Theory, **IT-24** (1978), 628-630.

27. N. Tokura, K. Taniguchi and T. Kasami, *A search procedure for finding optimum group codes for the binary symmetric channel*, IEEE Trans. Information Theory, **IT-13** (1967), 587-594.

28. T. J. Wagner, *A search technique for quasi-perfect codes*, Information and Control, **9** (1966), 94-99.

29. T. J. Wagner, *Some additional quasi-perfect codes*, Information and Control, **10** (1967), 334.

30. A. D. Wyner and J. Ziv, *On communication of analog data from a bounded source space,* Bell Syst. Tech. J., **48** (1969), 3139-3172 (see p. 3168, Lemma 2).

On the Covering Radius of Codes*

R. L. Graham
N. J. A. Sloane

Bell Laboratories
Murray Hill, NJ 07974

ABSTRACT

The covering radius R of a code is the maximal distance of any vector from the code. This paper gives a number of new results concerning $t[n, k]$, the minimal covering radius of any binary code of length n and dimension k. For example $t[n,4]$ and $t[n,5]$ are determined exactly, and reasonably tight bounds on $t[n, k]$ are obtained for any k when n is large. These results are found by using several new constructions for codes with low covering radius. One construction, the amalgamated direct sum, involves a quantity called the norm of a code. Codes with norm $\leq 2R+1$ are called normal, and may be combined efficiently. The paper concludes with a table giving bounds on $t[n, k]$ for $n \leq 64$.

* This appeared in ''IEEE Trans. Information Theory'', vol. 31 (1985), pp. 385–401.