Covering Radius—Survey and Recent Results

GÉRARD D. COHEN, MEMBER, IEEE, MARK G. KARPOVSKY, MEMBER, IEEE, H. F. MATTSON, JR., MEMBER, IEEE, AND JAMES R. SCHATZ

Abstract—**All known results on covering radius are presented, as well as some new results. There are a number of upper and lower bounds, including asymptotic results, a few exact determinations of covering radius, some extensive relations with other aspects of coding theory through the Reed–Muller codes, and new results on the least covering radius of any linear $[n, k]$ code. There is also a recent result on the complexity of computing the covering radius.**

I. INTRODUCTION

THE COVERING RADIUS of a block code of length n is defined as the smallest integer ρ such that all vectors in the containing space are within Hamming distance ρ of some codeword. Thus, for the binary case, the covering radius $t(C)$ of C is

$$t(C) = \max\{\min\{|x + c|;\ c \in C\};\ x \in Z_2^n\} \quad (1)$$

We restrict attention to binary codes except when we discuss Reed–Solomon codes and, briefly, one or two other cases. We assume no coordinate is identically zero.

The covering radius is a basic geometric parameter of a code, important, for example, in these respects.

1) It is a measure of the quality of a code in that *maximal* codes C, i.e., those having no proper supercode with the same length and minimum distance, are characterized by the condition $t(C) \leq d(C) - 1$. The proof is at the end of Subsection A, following.

2) Define $d[n, k]$ to be the largest minimum distance attained by any linear $[n, k]$ code [17]. For all n, k with $d[n, k] > d[n, k + 1]$, we have $t[n, k] \leq d[n, k + 1]$, and the $[n, k, d[n, k]]$ codes are maximal (see Appendix A for the definition of $t[n, k]$). For the proof, see Section III-F.

3) If the code C is used for data compression, the covering radius is a measure of the maximum distortion [4]; if for error correction, then $t(C)$ is the maximum weight of a correctable random error.

4) The related problem of the covering radius of a lattice in Euclidean space has been addressed [61]. Such lattices have applications to quantization and to coding for the Gaussian channel [62], [63]. An application to speech processing is mentioned in [72].

5) Some nonlinear codes, such as the Kerdock code, are the union of a linear code with its cosets of maximum weight.

6) The covering radius is used to upperbound the weight of "zero neighbors" in a new decoding procedure set forth in [80].

A. The Translate Leader

When C is linear, $t(C)$ is the weight of a coset leader of greatest weight. Also, if H is any parity check matrix for C, then $t(C)$ is the least integer ρ such that every syndrome is a sum of some ρ or fewer columns of H. (By the term *syndrome* we mean a column vector of $n - k$ entries, where C is an $[n, k]$ code and H is an $(n - k) \times n$ matrix.) The least integer w allowing such a sum for the syndrome s is the weight of a leader of the coset associated with s.

More generally, $t(C)$ is the weight of a *translate leader* of greatest weight, where a *translate* of C is $x + C = \{x + c;\ c \in C\}$ for $x \in Z_2^n$, and any vector of minimum weight in a translate is called a *leader* of that translate. There is a simple criterion for x to be a translate leader. For convenience, we identify each vector with its support, which is the subset of coordinate places where the vector is one. Then x is a leader of $x + C$ if and only if

$$|x + c| \geq |x|, \qquad \text{for all } c \in C.$$

But

$$|x + c| = |x| + |c| - 2|x \cap c| \geq |x|,$$

and so our criterion, to be used in Section IV, is that x is a translate leader for C if and only if for all $c \in C$, $2|x \cap c| \leq |c|$.

To prove that a code C is maximal if and only if $t(C) \leq d(C) - 1$, let x be a vector at distance $t(C)$ from C. Then $d(C \cup \{x\}) = \min\{d(C), t(C)\} < d(C)$ if and only if C is maximal.

B. Other Related Quantities

Other quantities are related to the covering radius. The packing radius is always less than or equal to the covering radius of a code. (The terms "packing integer" and "covering integer" were introduced by Prange [45].) Also the

Manuscript received August 20, 1983; revised April 25, 1984. The material in this paper was presented in part at IEEE International Symposia, Grignano, Italy, 1979, and Les Arcs, France, 1982, and at the International Conference on Combinatorial Geometries and Their Applications, Rome, 1981.

G. D. Cohen is with ENST, 46 Rue Barrault, 75634 Paris Cedex 13, France.

M. G. Karpovsky is with the College of Engineering, Boston University, Boston, MA 02215, USA.

H. F. Mattson, Jr., is with the School of Computer and Information Science, Link 313, Syracuse University, Syracuse, NY 13210, USA.

J. R. Schatz is at 9427 Bullring Lane, Columbia, MD 21046, USA.

0018-9448/85/0500-0328$01.00

radius f of a code C defined as [30, p. 172]

$$f = \min\{\max\{|u - v|;\ v \in C\};\ u \in Z_2^n\}$$

bears a simple relationship to the covering radius, namely $f + t(C) = n$ [26, Eq. 59]. To prove this, we let $Q(\cdot)$ stand for the function $\max\{\min\{(\cdot);\ v \in C\};\ u \in Z_2^n\}$. Then $-f = Q(-|u - v|)$, so $n - f = Q(n - |u - v|) = Q(|\bar{u} - v|) = t(C)$, by (1). Here $\bar{u}$ is the complement of u.

C. Outline of Paper

Our original intention was to survey all known results on covering radius, but in the process of organizing them we found, and have included here, some new results as well. They are found in Lemma 1, Proposition 1 (more on the supercode lemma), Equation (4), and Lemma 2 (all in Section III). Another result, on leader codes of second-order Reed–Muller codes, appears in Theorem 11 (Section IV). Section IV-C presents a characterization of "structure codes." Sections V and VI introduce and study an entirely new function of interest on which asymptotic results appear in Section VII and a table of values in Appendix B. A new result of Tietevainen is mentioned in Theorem 16 (Section VIII).

The plan of the paper is the following. Lower and upper bounds on covering radius are given in Sections II and III, respectively. Section IV gives covering radius results for Reed–Muller codes, and Section V deals with the least covering radius of (n, K) codes. In Section VI, $t[n, k]$ is determined for small k. The asymptotic results mentioned above are presented in Section VII, and Section VIII provides some additional, miscellaneous results. Finally, in Section IX, we give some open problems. In addition, Appendix B provides some codes of known covering radius and the table of values of $t[n, k]$ for $n \le 32$ and $k \le 25$.

Appendix A provides a list of the nomenclature used throughout this work.

II. Lower Bounds on Covering Radius

A. Perfect Codes and Quasi-perfect Codes

For any code C, we define

$$\Delta(C) = t(C) - e(C) \ge 0.$$

C is called perfect [quasi-perfect] if and only if $\Delta(C) = 0$ [$= 1$]. A result on $\Delta(C)$ for large n appears in Theorem 14 (Section VII). For each of the bounds below one can easily find a code meeting it with equality.

B. Sphere-Packing and Sphere-Covering Bounds

Theorem 1: For any (n, K) code C

$$\sum_{0 \le i \le e(C)} \binom{n}{i} \le 2^n/K \le \sum_{0 \le i \le t(C)} \binom{n}{i}.$$

The latter bound, first remarked in [54], is called the *sphere-covering bound*. If the linear code C is even, then half of its cosets have odd weight and half have even weight. Therefore both

$$\sum_{2i \le t(C)} \binom{n}{2i} \ge 2^{n-k-1} \qquad \sum_{2i+1 \le t(C)} \binom{n}{2i+1} \ge 2^{n-k-1} \tag{2}$$

must hold for even linear codes C [2].

We now derive lower bounds on the covering radii of codes constructed in various ways from two other codes. Let C_1 and C_2 be $[n_1, k_1, d_1]$, and $[n_2, k_2, d_2]$, codes, respectively, with generator matrices G_1 and G_2.

C. The Cartesian Product

Define $C = C_1 \times C_2 = \{(a, b);\ a \in C_1,\ b \in C_2\}$. Then C, the *Cartesian product* or *external direct sum* of C_1 and C_2, is a code of type $[n_1 + n_2, k_1 + k_2, \min\{d_1, d_2\}]$, and

$$t(C) = t(C_1) + t(C_2).$$

D. Catenation $C_1 + C_2$ of C_1 and C_2

Here we take $k_1 \le k_2$ and define the generator matrix of C as G_1', G_2, where G_1' is G_1 with $k_2 - k_1$ rows of zeros attached. This construction may give different codes C as one chooses different generator matrices for the same codes C_1 and C_2. C is an $[n_1 + n_2, k_2, d]$ code, where $d \ge \min\{d_1, d_2\}$, for which the covering radius satisfies

$$t(C) \ge t(C_1) + t(C_2).$$

E. $(u, u + v)$ Construction [30, Ch. 2, Sec. 9]

If $n_1 = n_2$, and $C_2 \subseteq C_1$, then C is defined as

$$C = \{(u, u + v);\ u \in C_1,\ v \in C_2\}.$$

C is a code of type $[2n_1, k_1 + k_2, \min\{2d_1, d_2\}]$, and $t(C) \ge 2t(C_1)$.

To verify this bound on $t(C)$, let a be a coset leader of C_1 of maximum weight. Then (a, a) is a coset leader for C, and $|(a, a)| = 2t(C_1)$.

F. Direct (Kronecker) Product [30, p. 568]

The direct product of the codes C_1 and C_2 produces an $[n_1n_2, k_1k_2, d_1d_2]$ code C for which the covering radius satisfies

$$t(C) \ge \max\{n_1t(C_2), n_2t(C_1)\}.$$

G. Lengthening a Code

It is always possible to adjoin another column h to the $k \times n$ generator matrix G of an $[n, k]$ code C. Then G becomes $G; h$, where h is a $k \times 1$ vector; the latter is the generator matrix of an $[n + 1, k]$ code C'. Obviously, the covering radius of C' is either the same as or one greater than that of C. Consider, for example, the $(2^m - 1, m)$ simplex code, with covering radius $2^{m-1} - 1$. Imagine constructing it one coordinate at a time, starting from the generator matrix I_m. As we "add" $2^m - m - 1$ columns, the covering radius increases from 0 to $2^{m-1} - 1$; thus

slightly more than half of the time, the increase is by one. The following result gives a criterion for this situation. Since the new column h is another parity check, the vectors of C' have the form $(c, c \cdot b)$, where $c \in C$ and b is a fixed vector of length n.

Lemma 1: When the $[n, k]$ code C is lengthened to an $[n+1, k]$ code C' via a new parity check b, then $t(C') = 1 + t(C)$ if and only if in some coset $u + C$ of coset weight $t(C) = |u|$, all coset leaders v satisfy $(u + v) \cdot b = 0$.

Proof: For any distinct cosets $x + C$ and $y + C$, the four C'-cosets of $(x, 0)$, $(x, 1)$, $(y, 0)$, and $(y, 1)$ are mutually distinct. With u as given, the vector $(u, 1)$ is a leader if and only if for all $c \in C$, $|(c, c \cdot b) + (u, 1)| = |c + u| + |c \cdot b + 1| \geq |u| + 1$, a condition holding automatically except perhaps when $u + c$ is a leader v of the coset. If and only if $c \cdot b = 0$ for all leaders v, $(u, 1)$ is a leader.

Corollary 1: Appending an overall parity check or the zero parity check increases the covering radius by one (cf. [2]). Puncturing a code on p coordinates reduces the covering radius by at most p.

Application of Lemma 1: Appending any nonzero column to the generator matrix of the simplex code leaves the covering radius unchanged. This is true because there is only one coset of maximum weight for the simplex code [34]; its leaders are the complements of all the nonzero codewords. Thus the $u + v$ of the lemma runs over all nonzero codewords, forcing b to be zero. (Here the overall parity check is the zero parity check.)

If, however, we delete any column from the generator matrix of the simplex code, then the covering radius decreases by one, because the code is even; i.e., the deleted column is an overall parity check on the remaining.

Another application is a simple bound for even binary codes C [2]: $t(C) \geq d/2$ for any $[n, k, d]$ code in which all weights are even, and equality holds iff C is the extension of a perfect code by an overall parity check. One proves the second part by puncturing C on one nonzero coordinate to get a code C' that satisfies

$$t(C') = t(C) - 1 = \frac{d}{2} - 1 = \left\lfloor \frac{d-2}{2} \right\rfloor = e(C').$$

The bound appears weak because it merely says that the code is not perfect, but it can be useful (see [2]).

The criterion of Lemma 1 can be restated (in the notation of the lemma) as follows.

Restatement: $t(C') = t(C)$ iff every coset of highest weight for C has coset leaders u, v such that $(u + v) \cdot b = 1$.

Corollary 2: If some coset of C of highest weight has a unique leader, then $t(C') = t(C) + 1$ (whatever b is).

Finally, because the proof of Lemma 1 did not use the fact that $|u| = t(C)$, it in fact states a criterion for $(u, 1)$ to be a coset leader of C' when u is a coset leader of C.

H. The Supercode Lemma

We now define two quantities associated with codes $C_1 \subset C_2$. We say $m(C_2, C_1)$ $[M(C_2, C_1)]$ is the weight of a translate-leader of least nonzero [greatest] weight among the translates of C_1 by elements of C_2:

$$m(C_2, C_1) = \min \{|x + c|;\ x \in C_2 - C_1,\ c \in C_1\}$$
$$M(C_2, C_1) = \max_{x \in C_2} \min \{|x + c|;\ c \in C_1\}. \quad (3)$$

When C_1 and C_2 are linear, these are the minimum nonzero and maximum weights of cosets of $C_2 \bmod C_1$.

Proposition 1 (The Supercode Lemma): Let C_1 and C_2 be possibly nonlinear codes such that $C_1 \subset C_2$. Then $t(C_1) \geq M(C_2, C_1) \geq m(C_2, C_1) \geq d(C_2)$. If both codes are linear, then, in particular,

$$t(C_1) \geq \min \{|x|;\ x \in C_2 - C_1\}.$$

Proof: Since $t(C_1)$ is by definition $\max \{wt(y + C_1);\ y \in Z_2^n\}$, we see that

$$t(C_1) = M(Z_2^n, C_1) \geq M(C_2, C_1).$$

The third inequality follows from the fact that $\mathrm{wt}(x + C_1)$ for $x \in C_2 - C_1$ is a nonzero distance in C_2. When both codes are linear, $m(C_2, C_1)$ reduces to the quantity stated in Proposition 1.

A special case of this useful result first appeared in [15]. It was also used in [21] to show that no e-error-correcting BCH code BCH (e) for $e \geq 3$ is quasi-perfect, settling a question raised in [15]: The BCH codes are nested, as

$$\mathrm{BCH}(1) \supset \mathrm{BCH}(2) \supset \mathrm{BCH}(3) \supset \cdots.$$

When the inclusion is proper we may apply the supercode lemma to see that

$$t(\mathrm{BCH}(2)) \geq d(\mathrm{BCH}(1)) = 3$$
$$t(\mathrm{BCH}(3) \geq d(\mathrm{BCH}(2)) = 5, \cdots.$$

The usefulness of the supercode lemma is explained in part by the following.

Remark: If C_1 is a code for which $t(C_1) \leq d(C_1)$, then there is a supercode C_2 for which $t(C_1) = d(C_2)$. To see this, just let x be any vector at distance $t(C_1)$ from C_1, and define C_2 as the supercode $C_1 \cup (x + C_1)$.

These conditions hold for all the Reed–Solomon codes, for which we now find the covering radii. These are $[n, k, n - k + 1]$ nonbinary codes [14, p. 21], [30, p. 294], [47] which are nested: for fixed q and $n \leq q - 1$, there are codes $C_0 \subset C_1 \subset C_2 \subset \cdots \subset C_n$, where C_i is an $[n, i, d_i]$ code over GF(q) with $d_i = n - i + 1$ for $1 \leq i$. It follows that $t(C_i) \geq d_{i+1} = n - i$ for all $i < n$. The reverse inequality follows from the redundancy bound (Section III-A). Thus, any Reed–Solomon code of distance d has covering radius $d - 1$, which equals the redundancy of the code.

It is not necessarily true that the covering radius equals the redundancy for any MDS code, however [30, Ch. 11]. Over GF(5) the [6, 4, 3] MDS code with check matrix [30, p. 323]

$$\begin{matrix} 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 2 & 3 & 4 & 0 & 1 \end{matrix}$$

has covering radius 1 but redundancy 2.

Finally, we present a simple example showing that all four quantities in the statement of the supercode lemma (Proposition 1) can be different from each other. Let A

and B be, respectively, (n, k, d) and (n', k', d') codes with $d < d' < w \leq n'$, where w is the maximum weight of codewords of B, and $k < n$. For C_2 take $A \times B = \{(a, b); a \in A, b \in B\}$, and for C_1 take $\{(a, 0); a \in A\} \subseteq C_2$. Then the coset space C_2/C_1 is isometric to B, so we see from Corollary 1 that

$$t(C_1) = n' + t(A) > w = M(C_2, C_1) > d' = m(C_2, C_1) > d = d(C_2).$$

III. Upper Bounds on Covering Radius

A. The Redundancy and Delsarte Bounds

The first and simplest bound on covering radius is given by the following proposition.

Proposition 2: The linear $[n, k]$ code C satisfies $t(C) \leq n - k$.

Proof: The proof is obvious if we recall that $t(C)$ is the least integer w such that every syndrome is a sum of at most w columns of the parity check matrix H of C, and H has rank $n - k$.

Notice that Reed–Solomon codes meet this bound with equality. (See the Remark, and text following, at the end of the previous section.)

Proposition 3: The bound $t(C) \leq n - k$ does not hold for nonlinear (n, K, d) codes in general (where $k = \log K$), but it does hold for maximal codes.

Proof: If C is maximal, then $t(C) \leq d - 1$ (See paragraph 1) at the beginning of the Introduction.) But $d - 1 \leq \lfloor n - k \rfloor$, the Singleton bound [51]. For the general case let n be odd and let C be the sphere of radius $n/2$ about 0. Then $|C| = 2^{n-1}$, so $n - k = 1$; but $t(C) = (n + 1)/2$.

Theorem 2 (Delsarte's Theorem [12]): Let s' be the external distance of the code C. If C is linear, s' is the number of nonzero weights in $C^{\perp}$; and if C is nonlinear, s' is defined analogously through the MacWilliams transform (see [12], [30, Ch. 5]). Then

$$t(C) \leq s'.$$

No proof of this result will be given here. Five proofs have appeared: [12], [1], [30, p. 172] and, for the linear case, [58], [2].

Remark: There are several classes of codes for which Delsarte's bound gives the exact value of the covering radius. Some of these are the perfect codes, the Reed–Muller codes $\mathrm{RM}(r, m)$ for $m - 3 \leq r \leq m$, the $\mathrm{BCH}(e)$ codes for $e = 1$, and for $e = 2$ and 3 with m odd [25], and the Reed–Solomon codes. (See also Section VIII-D.) But there is some slight evidence (see [31]) that the Delsarte bound is not very good for most codes.

B. The Supercode Upper Bound

Theorem 3: Let $C_1 \subset C_2$ be codes. Then $t(C_1) \leq t(C_2) + M(C_2, C_1)$, where M is defined as in Section II-H.

Proof: Let v be a vector in Z_2^n at distance $t(C_1)$ from C_1, and a a word in C_2 closest to v. Then $|a + v| \leq t(C_2)$. Let b be a word in C_1 closest to a. Then $|a + b| \leq M(C_2, C_1)$. It follows that

$$t(C_1) \leq |b + v| \leq |a + v| + |a + b| \leq t(C_2) + M(C_2, C_1).$$

Corollary 3: With C_2/C_1 as defined in Appendix A,

$$\max_{C_2 \supset C_1} \min_{x \in C_2 - C_1} |x| \leq t(C_1) \leq \min_{C_2 \supset C_1} \max_{x \in C_2 - C_1} |x| + t(C_2).$$

We now give an upper bound for codes constructed as in Section II-D from two linear codes C_1 and C_2, of lengths n_1 and n_2, respectively.

Proposition 4: Let C be any catenation of C_1 and C_2. Then

$$t(C) \leq \min\{t(C_1) + n_2, t(C_2) + n_1\}.$$

C. The $\rho_1 + \rho_2$ Bound

This bound applies only to linear $[n, k]$ codes A. Take a parity check matrix H of A in the form $H = I_r, D$, where D is an $r \times k$ matrix of rank j, and $r = n - k$. Define A_1 as the code of type $[k, k - j]$ with $D = pcm(A_1)$, and set $\rho_1 = t(A_1)$. Define A_2 as the $[r, j]$ code spanned by the columns of D, and set $\rho_2 = t(A_2)$.

Theorem 4 [31]: $t(A) \leq \rho_1 + \rho_2 = t(A_1) + t(A_2) \leq n - k$.

Proof: If x is any syndrome, then it is at distance ρ_2 or less from some vector y in A_2. Thus $x = y + z$, where z is the sum of at most ρ_2 columns of I_r. The set of all subsets of columns of D with sum y corresponds to a coset of A_1. Thus y is the sum of at most ρ_1 columns of D. Since $\rho_1 \leq j$ and $\rho_2 \leq r - j$ (see Section III-A), $\rho_1 + \rho_2 \leq r = n - k$.

With the same notation we can prove the following theorem.

Theorem 5 [33]: Let W be largest weight less than $r + \rho_1$ of any codeword of A. Then

$$t(A) \leq \lfloor W/2 \rfloor + \rho_2.$$

We omit the proof of this result. Sometimes Theorem 5 gives a better bound than Theorem 4. Both sometimes yield better bounds than the Delsarte bound [31], [33] where, in fact, sometimes the external distance is greater than the redundancy. These suffer, though because they bound covering radius in terms of covering radius, a difficult quantity to compute. The quantities j, ρ_1, and ρ_2 are not invariants of A. Finally, there are situations in which ρ_1 or ρ_2 can be found by inspection.

Similarly, let C be a nonlinear (n, k) code. Then the linear $[n + k, k]$ code A with parity check matrix I_n, D, where the columns of D are all the words of C, has covering radius satisfying

$$t(A) \leq 1 + t(C). \tag{4}$$

D. The Norse Bounds

The more complicated "Norse bounds," as we call them, hold for restricted classes of codes, which may, however, be nonlinear.

Definition: A code has *strength* s if and only if every s-subset of coordinate places contains every binary s-tuple the same number of times. A code is *self-complementary* if and only if the complement of every codeword is also a codeword.

Theorem 6 [18]: If the code C of length n has strength 1, then $t(C) \leq \lfloor n/2 \rfloor$.

Theorem 7 [18]: If the code C of length n has strength 2 and is self-complementary, then $t(C) \leq \lfloor (n - \sqrt{n})/2 \rfloor$.

These two bounds are asymptotically the same. In [18] Theorem 7 is applied to the first-order Reed–Muller code, yielding a bound we use in Section V-B. These bounds appear to be best for codes of low rate.

E. Code C' Where $t(C') \leq 1 + t(C)$

Lemma 2: Let C be an $[n, k, d]$ code with distance $d \leq 3$, and let $\{h_1, \cdots, h_n\} = H$ be the columns of a check matrix of C. Suppose, as we may, that $h_1 = 0$ if $d = 1$, $h_1 = h_2$ if $d = 2$, and $h_1 = h_2 + h_3$ if $d = 3$. Then the $[n + 2, k]$ code C' with check matrix

$$H' = \begin{matrix} 1 & 0 & 1 & \\ 0 & 1 & 1 & 0 \\ 0 & 0 & h_1 & h_2 \cdots h_n \end{matrix}$$

satisfies $t(C') \leq 1 + t(C)$.

Proof: Denote the first three columns of H' by c_1, c_2, c_3, respectively. If S is any set of column vectors of $n - k$ rows, denote by S' the same set with two extra zeros on top of each vector: $S' = \{(00y^T)^T;\ y \in S\}$. For such S (S') let ΣS ($\Sigma S'$) denote the sum of all elements of S (S').

We let s be any syndrome and divide the proof into the three cases:

$$s = \begin{matrix} \text{Case 1} & \text{Case 2} & & \text{Case 3} \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ x & x & x & x \end{matrix},$$

where x is any syndrome for C.

Case 1: Here we consider a smallest set S of columns h_i such that $x = \Sigma S$. If $h_1 \notin S$, then $s = \Sigma S'$ expresses s as a sum of $|S|$ columns of H'. If $h_1 \in S$, then when $d = 3$ we remove h_1 from S and insert h_2 and h_3; when $d = 2$ we replace h_1 by h_2; when $d = 1$, h_1 cannot be in S.

Case 2: Again express $x = \Sigma S$ for a smallest $S \subseteq H$. If $h_1 \notin S$, then $s = c_1 + x'$ (or $c_2 + x'$). But if $h_1 \in S$, then $s = c_i + c_3 + \Sigma S_1'$, where $S_1 = S - \{h_1\}$, for $i = 1$ or 2.

Case 3: Here we pick a smallest set $S \subseteq H$ such that $x + h_1 = \Sigma S$. If $h_1 \notin S$, then $s = c_3 + \Sigma S$. If $h_1 \in S$, then $s = c_1 + c_2 + \Sigma S_1'$, where $S_1 = S - \{h_1\}$.

In all cases we express s as a sum of at most $1 + t(C)$ columns of H'.

Notice that we used the hypothesis $d \leq 3$ only in Case 1 and when $h_1 \in S$. If we knew that our code C had for each coset of maximum weight a leader not having a 1 "at" h_1, then we could omit any restriction on d.

We shall use Lemma 2 in Section V.

F. Some Links Between $t(C)$ and $d(C)$.

We have noted in the Introduction that $t(C) \leq d(C) - 1$ holds if and only if C is maximal. We present here an improvement of this bound in a special case. We define $d[n, k]$ as in Section I. Then we have the following.

Proposition 5: If $d[n, k] > d[n, k + 1]$, then $t[n, k] \leq d[n, k + 1]$, and all $[n, k, d[n, k]]$ codes are maximal.

Proof: Let A be an $[n, k, d[n, k]]$ code. Let x be a coset leader for A of weight $t(A)$. Then $A \cup (x + A)$ is an $[n, k + 1, t(A)]$ code; thus

$$t[n, k] \leq t(A) \leq d[n, k + 1] \leq d[n, k] - 1.$$

A is maximal because $t(A) \leq d(A) - 1$.

IV. Covering Radius Results for Reed–Muller Codes

A. Bounds on Covering Radii

In this section we present some bounds on the covering radii of Reed–Muller codes and summarize the cases where exact results are known. $R(r, m)$ will denote the rth order Reed–Muller code of type $[2^m, \Sigma_{0 \leq i \leq r} \binom{m}{i}, 2^{m-r}]$. Let $\rho(r, m)$ denote the covering radius of $R(r, m)$.

$R(m, m)$ is simply the entire space of binary 2^m-tuples, so $\rho(m, m) = 0$. $R(0, m)$ consists of zero and the all-one vector, if $m \geq 1$, so $\rho(0, m) = 2^{m-1}$. Almost as trivial is the code $R(m - 1, m)$, which consists of all even weight binary 2^m-tuples. Clearly, $\rho(m - 1, m) = 1$. Since $R(m - 2, m)$ is an extended Hamming code our earlier remark (Corollary 1) about overall parity checks shows that $\rho(m - 2, m) = 2$. So much for the easy cases.

McLoughlin [37] determined the exact value of $\rho(m - 3, m)$. Her theorem, that

$$\rho(m - 3, m) = \begin{cases} m + 2, & m \text{ even} \\ m + 1, & m \text{ odd}, \end{cases} \tag{5}$$

is proved in two parts. First, an upper bound on $\rho(m - 3, m)$ is obtained by using Delsarte's theorem. This results from an upper bound on the number of nonzero weights in the dual code $R(m - 3, m)^{\perp} = R(2, m)$ found by Kasami [25]. Next, an elegant construction produces a coset in which the minimum weight meets this upper bound, and the result follows. It also shows that Kasami's upper bound is the exact value, which became known when the weight distribution of $R(2, m)$ was calculated [52].

Small Values of r: For small values of r less is known. When m is even, $\rho(1, m) = 2^{m-1} - 2^{(m-2)/2}$; for odd m,

$$2^{m-1} - 2^{(m-1)/2} \leq \rho(1, m) \leq 2^{m-1} - 2^{(m-2)/2}.$$

The lower bound comes from the supercode lemma (Proposition 1) and [25], [52]; the upper bound comes from [18]. Aside from this there are a few isolated cases: $\rho(1, 3) = 2$ (trivial); $\rho(1, 5) = 12$, due to Berlekamp and Welch

[6]; $\rho(1,7) = 56$, a highly nontrivial result due to Mykkeltveit [40]; $\rho(2,6) = 18$, due to Schatz [49]; $18 \le \rho(3,7) < 26$; and finally $\rho(1,15) \ge 2^{14} - 2^7 + 20$ and $\rho(1,2s+1) \ge 2^{2s} - 108 \cdot 2^{s-7}$ for $s \ge 7$ [42].

We now consider some bounds on $\rho(r,m)$.

Proposition 6: If $1 \le r \le m$ then

$$2\rho(r,m-1) \le \rho(r,m) \le \rho(r,m-1) + \rho(r-1,m-1)$$

and

$$\rho(r-1,m-1) \le \rho(r,m).$$

Proof: From the inductive definition of $R(r,m)$ [30, p. 374] we know that

$$R(r,m) = \{(u,u+v);\ u \in R(r,m-1),\ v \in R(r-1,m-1)\}.$$

Hence the result follows from Section II-E. The same inductive construction applied to the parity check matrices yields the last bound of Proposition 6, which in particular implies $18 \le \rho(3,7)$.

Our next theorem is a generalization of a result of McLoughlin [37].

Theorem 8: If $0 \le r \le m-3$, then

$$\rho(r,m) \ge \begin{cases} 2^{m-r-3}(r+4), & r \text{ even} \\ 2^{m-r-3}(r+5), & r \text{ odd} \end{cases}.$$

Proof: Let $t = m - r$. We prove the theorem by induction on t. If $t = 3$, then the bound follows from McLoughlin's result on $\rho(m-3,m)$. Now assume that there is a fixed $t \ge 3$ such that the bound holds whenever $0 \le r \le m-3$ and $m - r = t$. Suppose $0 \le r \le m-3$ and $m - r = t + 1$. Then $(m-1) - r = t$, so by inductive hypothesis and Proposition 6 we have

$$\rho(r,m) \ge 2\rho(r,m-1) \ge 2\begin{cases} 2^{(m-1)-r-3}(r+4), & r \text{ even} \\ 2^{(m-1)-r-3}(r+5), & r \text{ odd} \end{cases}.$$

Hence the result holds for all r and m with $0 \le r \le m-3$.

For the next theorem we assume that the reader is familiar with the basic properties of cyclic codes.

Theorem 9: If $m \ge 6$ and $2 \le r \le m-3$, then

$$\rho(r,m) \ge 2^{m-r}$$

Proof: Let α be a primitive element of GF(2^m). $R(r,m)^*$ (the punctured Reed–Muller code) is a cyclic code with zeros α^s for all s such that $1 \le s \le 2^m - 2$ and $1 \le w_2(s) \le m - r - 1$, where $w_2(s)$ is the number of ones in the binary expansion of s. (A proof of this fact is given in [30, p. 382].) Let $B(r,m)^*$ denote the binary BCH code of length $2^m - 1$ with zeros α^t for all $t = 1, 2, \cdots, 2^{m-r} - 2$. By the BCH bound, $B(r,m)^*$ has minimum distance at least $2^{m-r} - 1$. However, it is clear that $R(r,m)^* \subseteq B(r,m)^*$ so $B(r,m)^*$ has minimum distance $2^{m-r} - 1$.

Now, if $B(r,m)^*$ is a proper supercode of $R(r,m)^*$, then the supercode lemma (Section II-H) implies that $R(r,m)^*$ has covering radius at least $2^{m-r} - 1$, and so $\rho(r,m) \ge 2^{m-r}$ from Corollary 1. We claim that when $m \ge 6$ and $2 \le r \le m-3$, $B(r,m)^*$ is a proper supercode of $R(r,m)^*$. It suffices to prove that there exists a binary m-tuple $s = (s_0, \cdots, s_1)$ with $1 \le w_2(s) \le m - r - 1$ and such that the associated integer value of s, and each cyclic shift of s, is at least 2^{m-r}. (Such an s and its cyclic shifts correspond to α^s and the set of all conjugates of α^s; the properties sought for show that these are roots of the generator polynomial of $R(r,m)^*$ but not of $B(r,m)^*$.)

Let $m = qr + k$, $0 \le k < r$. We define

$$a = 1\ 0 \cdots 0\ \underbrace{}_{k}\ 1\ 0 \cdots 0\ \underbrace{}_{r}\ 1\ 0 \cdots 0\ \underbrace{}_{r} \cdots 1\ 0 \cdots 0\ \underbrace{}_{r},$$

where a contains q blocks of length r. Since the length of any string of zeros is at most $r - 1$, the integer value of a and all its cyclic shifts is at least 2^{m-r}. To finish the proof, we must show that if $k \ge 0$, then $q + 1 \le m - r - 1$, while if $k = 0$, then $q \le m - r - 1$. However, these results follow from the restrictions on m and r. This completes the proof.

Two comments are in order now. First, for $r \ge 5$, Theorem 9 yields a better bound than Theorem 8. Second, Theorem 9 shows that for $m \ge 6$, $2 \le r \le m-3$, $R(r,m)$ is a weak code in the sense that is a proper subcode of a code with the same minimum distance.

B. Other Results for $R(1,m)$ and $R(2,m)$

We now turn to some results of a different nature concerning $R(1,m)$ and $R(2,m)$. Theorem 10 below shows that the covering radius question for $R(1,m)$ is equivalent to an existence problem involving self-complementary binary linear codes. Theorem 11 extends these ideas in the direction of a necessary condition on the coset leaders of $R(2,m)$. We first list a few definitions and facts on Reed–Muller codes.

Form the $m \times 2^m$ matrix whose ith column is the binary expansion of i for $0 \le i \le 2^m - 1$. Adjoin a row of ones to obtain an $(m+1) \times 2^m$ matrix $M(m)$. Then $M(m)$ is a generator matrix for $R(1,m)$. For $m = 3$,

$$M(3) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

We identify vectors of length 2^m with their supports to get a one-to-one correspondence between subsets of the set GF$(2)^m$ of binary m-tuples and the set of binary vectors of length 2^m. An r-flat of GF$(2)^m$ is an r-dimensional subspace or a coset of such a subspace. The minimum-weight codewords in $R(r,m)$ are precisely the 2^m-long incidence vectors of the $(m-r)$-flats in GF$(2)^m$. This important fact is proved in [30, p. 380], for example. Finally, we recall that

a binary linear code is called self-complementary if it contains the all-one vector.

The following theorem is due to Mattson and Schatz [48], and independently to Mykkeltveit [40].

Theorem 10: $R(1, m)$ has a coset leader of weight n, with $2^{m-2} < n < 2^{m-1}$, if and only if there exists a self-complementary $[n, m+1, d]$ code C such that $d \geq n - 2^{m-2}$ and $d^{\perp} \geq 3$, where $d^{\perp}$ is the minimum distance of $C^{\perp}$.

Proof: Let n be a fixed integer such that $2^{m-2} < n < 2^{m-1}$, and let v be a coset leader of $R(1, m)$ with $\mathrm{wt}(v) = n$. The support of v selects n columns from $M(m)$, the generator matrix for $R(1, m)$. Let G denote the $(m+1) \times n$ matrix formed by these columns. Note that

$$G = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ & & T & & \end{bmatrix} \tag{6}$$

for some $m \times n$ matrix T. Let C be the code generated by G. C is called the *leader code* of v.

First note that C is self-complementary and $d^{\perp} \geq 3$ since the columns of G are distinct. Let x be the 2^m-tuple corresponding to an $(m-1)$-dimensional subspace X of $\mathrm{GF}(2)^m$, and let $\bar{x}$ be the complementary 2^m-tuple. Then $x, \bar{x} \in R(1, m)$ and, since v is a coset leader, we know from Section I-A that

$$\mathrm{wt}(v \cap x) \leq 2^{m-2} \tag{7}$$

Similarly,

$$\mathrm{wt}(v \cap \bar{x}) \leq 2^{m-2}. \tag{8}$$

Let c be any codeword of C other than 0 or **1** (the all-one vector.) There exists an $a \in \mathrm{GF}(2)^m$ such that either $c = aT$ or $c = aT + \mathbf{1}$. Assume that $c = aT$. Let x be the 2^m-tuple corresponding to the $(m-1)$-dimensional subspace $\{a\}^{\perp} = \{b \in \mathrm{GF}(2)^m;\ a \cdot b = 0\} = x$. A column t of T belongs to $\bar{X}$ if and only if $a \cdot t = 1$. Thus the weight of c can be expressed as

$$\mathrm{wt}(c) = \mathrm{wt}(v \cap \bar{x}) = n - \mathrm{wt}(v \cap x). \tag{9}$$

Using (7) and (8) we conclude that

$$n - 2^{m-2} \leq \mathrm{wt}(c) \leq 2^{m-2}. \tag{10}$$

Moreover, since $\mathrm{wt}(c + \mathbf{1}) = n - \mathrm{wt}(c)$, we have

$$n - 2^{m-2} \leq \mathrm{wt}(c + \mathbf{1}) \leq 2^{m-2}. \tag{11}$$

It follows from (10) and (11) that the minimum distance d of C satisfies $d \geq n - 2^{m-2}$. Since $n > 2^{m-2}$, it also follows that all nontrivial linear combinations of rows of T produce nonzero vectors of weight less than n. Hence C has dimension $m+1$.

Conversely, suppose that we are given a self-complementary $[n, m+1, d]$ code C with $d \geq n - 2^{m-2}$, $d^{\perp} \geq 3$, and $2^{m-2} < n < 2^{m-1}$. Then C has a generator matrix G of the form (6). G has distinct columns since $d^{\perp} \geq 3$. Let v be the 2^m-tuple that corresponds to the set of columns of G. We must show that $\mathrm{wt}(v + r) \geq \mathrm{wt}(v)$ for each $r \in R(1, m)$. Since $n < 2^{m-1}$, $\mathrm{wt}(v + \mathbf{1}) \geq \mathrm{wt}(v) = n$. For $r \neq 0, \mathbf{1}$ either $r = x$ or $r = \bar{x}$, where x is the 2^m-tuple corresponding to some $(m-1)$-dimensional subspace X of $\mathrm{GF}(2)^m$. We can express X as $\{a\}^{\perp}$ for some nonzero $a \in \mathrm{GF}(2)^m$. One easily reverses the arguments leading to (7), (8), (9), and (10) to show that $\mathrm{wt}(v + r) \geq \mathrm{wt}(v)$ for all $r \in R(1, m)$. This completes the proof.

The theorem above is the basis for Mykkeltveit's proof that $\rho(1, 7) = 56$. It was known that there exists a self-complementary $[56, 8, 24]$ code so $\rho(1, 7) \geq 56$ was clear. Mykkeltveit proved that $\rho(1, 7) = 56$ by showing that there does not exist a self-complementary $[57, 8, 25]$ code. The proof is difficult. The interested reader should see [40] for details.

Theorem 11: Let $m \geq 6$ and let $n \geq 2^{m-2}$. Suppose that v is a coset leader of $R(2, m)$ with $\mathrm{wt}(v) = n$. Let G be the matrix formed by the columns of $M(m)$ selected by v, and let C be the code generated by G. The C is a self-complementary $[n, m+1, d]$ binary linear code with $d \geq n - r$, where $r = \rho(1, m-1)$.

Proof: First note that since $m \geq 6$ there do exist coset leaders of weight 2^{m-2} by Theorem 9, so the assertion is not vacuous. Let v be as above. Let x and $\bar{x}$ be the 2^m-long incidence vectors of an $(m-1)$-dimensional subspace X of Z_2^m and its complement, respectively. Now $x, \bar{x} \in R(2, m)$ and again by Section I-A we have

$$\mathrm{wt}(v \cap x) \leq 2^{m-2} \tag{12}$$

$$\mathrm{wt}(v \cap \bar{x}) \leq 2^{m-2}. \tag{13}$$

We wish to improve these bounds.

Suppose that S is an $(m-2)$-dimensional subspace of Z_2^m such that $S \subseteq X$, and let the proper cosets of S be S_1, S_2, S_3, where $S_1 \subseteq X$, and S_2 and S_3 are contained in the complement $\bar{X}$ of X. The incidence vectors of these flats are denoted by s, s_1, s_2, and s_3, respectively. Now since s and s_i belong to $R(2, m)$, for $i = 1, 2, 3$, and since v is a coset leader, we obtain

$$\mathrm{wt}(v \cap s) \leq 2^{m-3} \tag{14}$$

and

$$\mathrm{wt}(v \cap s_i) \leq 2^{m-3}. \tag{15}$$

Regarding G as a set of columns, let w and z denote the 2^m-long incidence vectors of the sets $G \cap X$ and $G \cap \bar{X}$, respectively. Let f: $X \to Z_2^{m-1}$ be an isomorphism of vector spaces. Then each of the sets $f(S)$, $f(S_1)$, and $f(G \cap X)$ has a corresponding incidence vector of length 2^{m-1} denoted by s', s_1', and w', respectively. Moreover, by (12), (14), and (15) we have

$$\mathrm{wt}(w') = \mathrm{wt}(w) \leq 2^{m-2} \tag{16}$$

$$\mathrm{wt}(w' \cap s') = \mathrm{wt}(v \cap s) \leq 2^{m-3} \tag{17}$$

and

$$\mathrm{wt}(w' \cap s_1') = \mathrm{wt}(v \cap s_1) \leq 2^{m-3}. \tag{18}$$

But, the inequalities (16), (17), and (18) are equivalent to the inequalities $\mathrm{wt}(w' + 1) \geq \mathrm{wt}(w')$, $\mathrm{wt}(w' + s') \geq \mathrm{wt}(w')$, and $\mathrm{wt}(w' + s_1') \geq \mathrm{wt}(w')$, respectively. More-

over, these inequalities hold for any $(m-2)$-dimensional subspace S contained in X and its coset S_1 contained in X. It follows that w' is a coset leader of $R(1, m-1)$. Hence

$$\mathrm{wt}(v \cap x) = \mathrm{wt}(w') \leq \rho(1, m-1). \tag{19}$$

This improves the bound (12).

The improvement of the bound (13) proceeds in a similar manner, except that we first introduce a translation. That is, fix an element $a \in \bar{X}$ and define a map g: $\bar{X} \to S$ by $g(u) = u + a$. We now have

$$\bar{X} \xrightarrow{g} X \xrightarrow{f} Z_2^{m-1},$$

and both f and g are bijections. Applying the map fg to the sets S_2, S_3, and $G \cap \bar{X}$, we obtain subsets of Z_2^{m-1} whose length 2^{m-1} incidence vectors are denoted by s_2', s_3', and z', respectively. By (16) and (17) we have

$$\mathrm{wt}(z') = \mathrm{wt}(z) \leq 2^{m-2}$$
$$\mathrm{wt}(z' \cap s_2') = \mathrm{wt}(v \cap s_2) \leq 2^{m-3}$$
$$\mathrm{wt}(z' \cap s_3') = \mathrm{wt}(v \cap s_3) \leq 2^{m-3}.$$

Again, these inequalities are equivalent to $\mathrm{wt}(z' + \mathbf{1}) \geq \mathrm{wt}(z')$, $\mathrm{wt}(z' + s_2') \geq \mathrm{wt}(z')$, and $\mathrm{wt}(z' + s_3') \geq \mathrm{wt}(z')$. And, since these bounds hold for any $(m-2)$-flat S_2 contained in $\bar{X}$ and its complement S_3 contained in $\bar{X}$, it follows that z' is a coset leader of $R(1, m-1)$. Hence

$$\mathrm{wt}(v \cap \bar{x}) = \mathrm{wt}(z') \leq \rho(1, m-1). \tag{20}$$

We now use the fact that $\mathrm{wt}(v \cap \bar{x}) = n - \mathrm{wt}(v \cap x)$ together with (19) and (20) to obtain

$$n - r \leq \mathrm{wt}(v \cap \bar{x}) \leq r, \tag{21}$$

where $r = \rho(1, m-1)$. As we saw in the proof of theorem 10, the numbers $\mathrm{wt}(v \cap \bar{x})$ and $n - \mathrm{wt}(v \cap \bar{x})$ are precisely the weights of the codewords of C. Hence the minimum distance d of C satisfies $d \geq n - r$. Moreover, we have assumed that $2^{m-2} \leq n$ and that $\rho(1, m-1) < 2^{m-2}$ (for the latter, see "Small Values of r" in Subsection A, above). Hence, using (21), we can argue as in the previous proof that C has full dimension $m+1$. This completes this proof.

It is known [49] that $\rho(2, 6) = 18$. Hence Theorem 11 shows that a weight-18 coset leader of $R(2, 6)$ yields an $[18, 7, 6]$ code. For $m \geq 7$, $\rho(2, m)$ is unknown.

Theorem 10 is much more useful than Theorem 11 for demonstrating that certain codes exist. In fact, a unified approach to the existence of a large number of interesting codes can be based on the fact that $\rho(1, m)$ is known for all even m. It can be shown that the codes corresponding to maximum-weight coset leaders of $R(1, m)$ for even m have exactly three nonzero weights.

Theorem 12 [48]: For all even $m \geq 4$ there are $[n = 2^{m-1} - 2^{(m-2)/2}, m+1]$ codes with the following weight distributions:

weight	number of codewords
0	1
$2^{m-2} - 2^{(m-2)/2}$	$2^m - 1$
2^{m-2}	$2^m - 1$
n	1.

Many of these codes and their anticodes have the maximum d for the given n and k.

Bent functions are another approach to these ideas. If m is even, a bent function is defined as a polynomial in m variables $x_1, \cdots, x_m$ over Z_2 that (in effect) produces as its list of values over Z_2^m a vector of length 2^m that is a coset leader of maximum weight for the code $R(1, m)$. (See [30, Ch. 14.5] and [75], [76].) The code of Theorem 12 is the leader code of the support of a bent function.

Another use of bent functions is in [26], where it is proved that if the characteristic function $h(x_1, \cdots, x_{n-k})$ of the set of columns of the check matrix of the code C is bent, then $t(C) = 2$.

[136, 9, 64] Code: There is a [136, 9, 64] code; it has the largest minimum distance $d[136, 9]$ of all [136, 9] codes. It is constructed from the [120, 9] code of Theorem 12 as follows. We delete the all-one vector to get a [120, 8] code of two weights 56 and 64. Its anticode is therefore a [136, 8] code of weights 64 and 72. By adding the all-one vector, we make it a [136, 9, 64] code, optimal by the Griesmer bound.

Finally, $\rho(r, m)$ is known for all values of r when $m \leq 6$. The smallest Reed–Muller codes for which the covering radius is not known are $R(2, 7)$ and $R(3, 7)$.

C. Structure Codes

Consider the simplex code S_m of type $[2^m - 1, m, 2^{m-1}]$. If v is a coset leader of S_m, the *structure code* of v [53] is the orthogonal code of the leader code of v (cf. Section IV – B) generated by the submatrix of G_m (the generator matrix of S_m) the columns of which correspond to the support of v. The question posed in [53], to characterize the structure codes of coset leaders of S_m, and the analogous question for $R(1, m)$, are answered by Theorem 10, because it characterizes the leader codes.

Corollary 4 (Corollary to Theorem 10 [48]): The $[n, n-k, d]$ code A with $k \leq m$ and $d \geq 3$ is the structure code of a coset leader of S_m if and only if the maximum weight $\bar{d}$ in $A^{\perp}$ satisfies $\bar{d} \leq 2^{m-2}$.

A recasting of Theorem 10 yields the analogous result for the structure code of $R(1, m)$: the $[n, n-m-1, d]$ code B with $2^{m-2} < n < 2^{m-1}$ and $d \geq 4$ is the structure code of a coset leader of $R(1, m)$ if and only if B is even and $d(B^{\perp}) \geq n - 2^{m-2}$.

V. On the Least Covering Radius of (n, K) Codes

In this section we estimate the functions $t[n, k]$ and $t(n, K)$, defined as the least value of $t(C)$ as C runs over the class of, respectively, all binary linear $[n, k]$ codes and all binary (n, K) codes. As we shall see below, the codes

with the smallest covering radius do not necessarily have the largest packing radius.

A table of the function $t[n, k]$ for $n \leq 32$ and $k \leq 25$ is given in Appendix B.

A. Lower Bounds on $t[n, k]$ and $t(n, K)$

The sphere covering bound

$$\sum_{0 \leq i \leq t(n,K)} \binom{n}{i} \geq 2^n/K \tag{22}$$

leads to the following proposition.

Proposition 7: $t(n, K) \geq n/2 - 2^{-3/2}(Kn)^{1/2}$

Proof: Let the (n, K) code C have covering radius $t(n, K)$. Then (22) implies that for odd n

$$2^{n-1} - \sum_{i=1+t(n,K)}^{\lfloor n/2 \rfloor} \binom{n}{i} \geq 2^n/K.$$

In other words, $t(n, K) \geq \rho_0$, where ρ_0 is defined as the smallest integer for which

$$\sum_{\rho_0+1}^{n-1-\rho_0} \binom{n}{i} \leq 2^n - 2^{n+1}/K. \tag{23}$$

Now we estimate the sum in (23) by considering the random variable $\mathrm{wt}(x) = \mathrm{wt}(x_1, \cdots, x_n)$, where the x_i are independent random variables with $\Pr(x_i = 0) = \Pr(x_i = 1) = 1/2$, and wt is the Hamming weight function. Then $\mathrm{wt}(x)$ is binomial with $E(\mathrm{wt}(x)) = n/2$ and $\mathrm{var}(\mathrm{wt}(x)) = n/4$. Now (23) can be rewritten as

$$P = \Pr\left(|n/2 - \mathrm{wt}(x)| < n/2 - \rho_0\right) \leq 1 - 2/K.$$

To this we can apply the Bienaymé–Chebyshev inequality, that

$$\Pr\left(|V - E(V)| \leq \lambda\right) > 1 - \mathrm{var}(V)/\lambda^2,$$

where V is a random variable. By setting $V = \mathrm{wt}(x)$ and $\lambda = n/2 - \rho_0$, we get

$$1 - \frac{n/4}{(n/2 - \rho_0)^2} \leq P \leq 1 - 2/K,$$

from which the result follows. The case when n is even is similar.

The bound (22) is good, much better for covering radius than the sphere-packing bound is for packing radius. See Theorem 15 in Section VII for details.

Olson–Spencer and Beck–Fiala Bounds: Define $f(K)$ to be the smallest integer such that for all K-subsets L of Z_2^n there is a vector $x \in Z_2^n$ with $|x| \geq n/2$ such that for all $v \in L$, $||v \cap x| - |v \cap \bar{x}|| \leq f(K)$. (Here the outer vertical bars mean absolute value, and the inner ones mean the weight; we identify vectors with their supports, as before.) Since $|v \cap x| - |v \cap \bar{x}| = |x| - |x + v|$, the definition of $f(K)$ implies that for all $v \in L$,

$$|x + v| \geq n/2 - f(K).$$

Using estimates on $f(K)$ from [3] and [41], we have the following bounds on $t(n, k)$.

Olson–Spencer:

$$t(n, K) \geq n/2 - (2K)^{1/2} \log_e 2K.$$

Beck–Fiala:

$$t(n, K) \geq n/2 - 8(2K \log_e 2K)^{1/2}.$$

The Signature Bound: The following bound on $t[n, k]$ is useful when k is small. Recall that our codes have no coordinates identically zero.

Proposition 8: If $2 \leq k \leq 1 + \log n$, then $t[n, k] \geq \lceil n/2 \rceil - 2^{k-2}$.

Proof: Let C be an $[n, k]$ code with covering radius $t(C)$. For each $i = 1, \cdots, 2^k - 1$, denote by n_i the number of columns in a generator matrix G of C that represent the integer i in the base 2. Call the vector $\langle n_i \rangle$ the *signature* of the code. Now permute the columns of G so that $G = G_0, G_1$, where G_0 is a generator matrix of a code C_0 of signature $\langle 2\lfloor n_i/2 \rfloor \rangle$, and G_1 is that for C_1 of signature $\langle n_i - 2\lfloor n_i/2 \rfloor \rangle$. From Section II-D we see that $t(C) \geq t(C_1) + t(C_0)$. Now $C_0 = \Sigma R_i$, where the R_i are $[2\lfloor n_i/2 \rfloor, 1]$ repetition codes, so $t(C_0) \geq \Sigma t(R_i) = \Sigma \lfloor n_i/2 \rfloor$.

C_1 is the simplex code, punctured $m = 2^k - 1 - \Sigma(n_i - 2\lfloor n_i/2 \rfloor)$ times.

Hence from Corollary 1 we find that

$$\begin{aligned} t(C_1) &\geq 2^{k-1} - 1 - m \\ &= \sum (n_i - 2\lfloor n_i/2 \rfloor) - 2^{k-1} \\ &= n - 2^{k-1} - 2\sum \lfloor n_i/2 \rfloor. \end{aligned}$$

Now if $\Sigma \lfloor n_i/2 \rfloor \geq n/2 - 2^{k-2}$, which is nonnegative by hypothesis, then $t(C) \geq t(C_0) \geq n/2 - 2^{k-2}$. If however $\Sigma \lfloor n_i/2 \rfloor < n/2 - 2^{k-2}$, then

$$\begin{aligned} t(C) &\geq t(C_0) + t(C_1) \\ &\geq n - 2^{k-1} - \sum \lfloor n_i/2 \rfloor > n/2 - 2^{k-2}. \end{aligned}$$

To compare these lower bounds, we note that (22) can be used for any n and K. As we remark in Subsection B below (in regard to the nonconstructive upper bound), with $n < R \log K$ (R constant), (22) is asymptotically tight. Subsequent bounds can be used for small K and large n. If $k \leq 7$, then use Proposition 8; if $7 \leq k \leq 63$, use the Olson–Spencer bound; and for $64 \leq k$ use the Beck–Fiala bound. If $n < 32(k + 1)$, then Proposition 7 is better than the Beck–Fiala bound.

B. Upper Bounds for $t[n, k]$

All the upper bounds presented in this section are constructive except for (32).

First we note from the direct-sum construction (see Section II-C) that

$$t\left[\sum n_i, \sum k_i\right] \leq \sum t[n_i, k_i]. \tag{24}$$

In particular, $t[n, k] \leq t[n - 1, k - 1]$ and $t[n + 1, k] \leq 1 + t[n, k]$. Using Hamming codes and this bound, we

have

$$t\left[\sum(2^{n_i}-1), \sum(2^{n_i}-n_i-1)\right] \le q, \qquad (25)$$

where q is the number of summands.

We can always choose a parity check matrix in the form

$$H = I_r, 1^r, H',$$

where here 1^r stands for a column of r 1's, and $r = n - k$. Thus

$$t[n,k] \le \lceil (n-k)/2 \rceil. \qquad (26)$$

This simple bound in many cases gives the exact value of $t[n,k]$. We shall now improve it.

Proposition 9: Suppose that for a given k there are integers $n_1, \cdots, n_q$ such that

$$k > A = \sum_{1 \le i \le q} (2^{n_i} - n_i - 1).$$

Then $n \ge k$ implies

$$t[n,k] \le \left\lfloor \frac{1}{2}\left(n - k + 1 - \sum_{1 \le i \le q} n_i\right)\right\rfloor + q.$$

Proof: Set $B = k - A$. Then using (24)–(26) we see that for $B \ge 1$

$$\begin{aligned} t[n,k] &= t[n-k+A+B, A+B] \\ &\le t[n-k+A+1, A+1] \\ &= t\Big[n-k-\textstyle\sum n_i + 1 \\ &\quad + \textstyle\sum(2^{n_i}-1), \sum(2^{n_i}-n_i-1)+1\Big] \\ &\le t\Big[n-k+1-\textstyle\sum n_i, 1\Big] \\ &\quad + t\Big[\textstyle\sum(2^{n_i}-1), \sum(2^{n_i}-n_i-1)\Big] \\ &\le \left\lfloor \frac{1}{2}\left(n-k+1-\sum n_i\right)\right\rfloor + q. \end{aligned}$$

As a special case we get another upper bound for $t[n,k]$ by setting $q = 1$ if $k > 2^m - m - 1$, namely,

$$\begin{aligned} t[n,k] &\le \left\lfloor \frac{1}{2}(n-k+1-m)\right\rfloor + 1 \\ &\le \left\lfloor \frac{1}{2}(n-k+1-\lceil \log k \rceil\right\rfloor + 1. \qquad (27) \end{aligned}$$

Taking $n_i = m$ for all i, we have from Proposition 9 when $k > q(2^m - m - 1)$

$$t[n,k] \le \left\lfloor \frac{1}{2}(n-k+1-qm)\right\rfloor + q. \qquad (28)$$

We apply this bound, for example, to the case $n = 62$, $k = 52$, taking $q = 2$ and $m = 5$. From (28) and (22) we see that $t[62,52] = 2$. Notice that $t[62,51] \ge t[63,52] = 3$, by Sections II-B and C.

We may use codes other than Hamming codes when we specialize (24); for example, similar results arise when we replace some of the Hamming codes by Golay codes.

The bound (4) yields the following result on $t[n,k]$ if we choose for C a code of type $(n-k, K)$ of smallest covering radius. After replacing $n - k$ by n, we get

$$t[n+k, K] \le 1 + t(n, K). \qquad (29)$$

With (29) we could make a different proof of the upper bounds in Proposition 11 for $k = 4$.

Upper Bounds for $t[n,k]$ Based on First-Order Reed–Muller Codes $RM(1,m)$: Using $t[\mathrm{RM}(1,m)] \le 2^{m-1} - 2^{(m-2)/2}$ (Theorem 7), we deduce

$$t[n,k] \le \left(n - 2^{\lfloor \log n \rfloor/2} - k + \lfloor \log n \rfloor + 2\right)/2 \qquad (30)$$

for $n \le 2^{k-2}$. To see why this is so, one can write $n = (n - 2^{\lfloor \log n \rfloor}) + 2^{\lfloor \log n \rfloor}$ and $k = (k - \lfloor \log n \rfloor - 1) + \lfloor \log n \rfloor + 1$ and then use (24) and (26).

The bound (30) can be further improved if we use (28) instead of (26), but we do not state the result here.

For $n \ge 2^{k-2}$ we have the bound

$$t[n,k] \le \lfloor n/2 \rfloor - \lfloor 2^{(k-4)/2} \rfloor. \qquad (31)$$

To prove this, we set $m = k - 2$ and split n, k as $n = 2^m + (n - 2^m)$, $k = (m+1) + 1$. We note that these last two bounds are useful for large n.

Nonconstructive Upper Bound for $t[n,k]$: Using probability, we have found [9] an upper bound valid for all large n:

$$t[n,k] \le nH^{-1}(1 - k/n) + O(n^{-1}\log n). \qquad (32)$$

Here H^{-1} is the inverse function of $H(x) = -x\log x - (1-x)\log(1-x)$. If k/n has a limit $R > 0$, then (32) gives the exact asymptotic value:

$$t[n, Rn] \sim nH^{-1}(1-R). \qquad (33)$$

Comparing these upper bounds we see that they can be best used according to the following table.

Range of n	Appropriate Bound
$n \le$ (constant) k	(32)
$n \le k^2/4$	(26)–(29)
$k^2/4 \le n \le 2^{k-2}$	(30)
$2^{k-2} \le n$	(31)

VI. Determination of $t[n,k]$ for Small k

Proposition 10:

$$\begin{aligned} t[n,1] &= \lfloor n/2 \rfloor \\ t[n,2] &= \lfloor (n-1)/2 \rfloor, \qquad n \ge 2 \\ t[2s+1,3] &= s - 1, \qquad s \ge 1. \end{aligned}$$

Proof: We combine the lower bound from Proposition 8 with the upper bound (31).

Theorem 13: If $n > 2^k - \max\{2^{(k-2)/2}, k\}$, then $[n,k]$ codes C with $t(C) = t[n,k]$ and no columns of zeros in G are not projective (i.e., they have repeated columns in their generator matrices), and

$$t[n,k] \ge t[n-2,k] + 1.$$

Proof: If such a code C had no repeated columns, then it would be a punctured simplex code; by Corollary 1

we see that

$$t(C) \geq 2^{k-1} - 1 - (2^k - 1 - n) = n - 2^{k-1}.$$

Now also (31) and (26) tell us that

$$t(C) \leq \min\{n/2 - 2^{(k-4)/2}, (n-k)/2\}.$$

These inequalities contradict each other when n satisfies the hypothesis of Theorem 13. Now that there is at least one column appearing twice in G, we regard C as the catenation (Section II-D) of C_1 and C_2, where C_1 is a $[2,1]$ code and C_2 is an $[n-2, k']$ code with $k' \leq k$. From Section II-D we find that

$$t(C) \geq t(C_1) + t(C_2) \geq 1 + t[n-2, k],$$

where we have also used the obvious bound

$$t[n, k'] \geq t[n, k] \text{ if } k' \leq k.$$

We note that no $[n, k]$ code C with $t(C) = t[n, k]$ need have any column of zeros in its generating matrix; in fact, by Corollary 1, we might decrease $t(C)$ if we replace a column of zeros by a nonzero column.

Remark: An affirmative solution to problem 5) in Section X would imply that, under the same hypothesis on n, $t[n, k] = t[n-2, k] + 1$.

Proposition 11:

$$t[2s, 3] = s - 1$$
$$t[2s+1, 4] = s - 2 \text{ or } s - 1$$
$$t[2s, 4] = s - 2.$$

Proof: $t[6, 3] = 2$ implies $t[8, 3] \geq 3$, by Theorem 13; now, by iteration of Theorem 13 we get $t[2s, 3] \geq s - 1$. On the other hand, $t[2s, 3] \leq t[2s-1, 2] = s - 1$ by Proposition 10.

For $t[2s+1, 4]$ we have $t[11, 4] \geq 3$ by Section III-B, the sphere-covering bound. Using Theorem 13 repeatedly, as above, we find that $t[2s+1, 4] \geq s - 2$. For the upper bound we use $t[2s+1, 4] \leq t[2s, 3] = s - 1$.

We begin the final section of the proof by showing that

$$t[12, 4] = 4. \tag{34}$$

For if not, then $t[12, 4] = 3$, and there must be repeated columns in the generator matrix of a $[12, 4]$ code C with $t(C) = 3$, for otherwise C is the $[15, 4]$ simplex code punctured three times, so $t(C)$ would be at least $7 - 3 = 4$. Therefore $t[12, 4] \geq t[10, 4] + 1 = 4$ by Theorem 13. It follows that $t[2s, 4] \geq s - 2$ for all $s \geq 2$. But from (26) we get the reverse inequality.

Proposition 12: $t[2s, 5] \leq s - 3$ if $s \geq 4$ and $t[2s+1, 5] \leq s - 2$ if $s \geq 2$.

Proof:

$$t[2s, 5] \leq t[2s-7, 1] + t[7, 4] \leq s - 3;$$
$$t[2s+1, 5] \leq t[2s, 4] \leq s - 2.$$

VII. Asymptotic Results

Theorem 14: For each $i \geq 1$ let C_i be an (n_i, K_i) code such that $n_i \to \infty$. If the information rate $\log K_i / n_i$ is bounded away from zero and one, then there is a constant $b > 0$ such that $\Delta(C_i) \geq b \cdot n_i$ for all sufficiently large i [32].

Proof: The sphere-covering lower bound on $t(C_i)/n_i$ for large n is strictly above the Elias or McEliece *et al.* upper bounds on $e(C_i)/n_i$. See [43, p. 79] or [5, p. 302] or [30, p. 564].

Corollary 5: Define $e[n, k]$ to be the largest packing radius of any $[n, k]$ code. Then if k/n is bounded away from 0 and 1,

$$t[n, k] - e[n, k] = O(n).$$

Theorem 15 [9]: For all n, k such that $2 \log n < k < n$, the $[n, k]$ codes C satisfy

$$t(C) \leq nH^{-1}(1 - k/n + 2 \log n/n)$$

for at least the proportion $1 - 2^{-k}$ of such codes.

The asymptotic form of this result shows that the sphere-covering bound is good: for constant R, $0 < R < 1$ and all large n,

$$t(n, nR) \sim nH^{-1}(1 - R).$$

Proposition 13 [10]: Let $e \geq 2$. For all sufficiently large n, it is true that

$$t[n, n - \lceil e \log n \rceil] = e + 1.$$

For example, for large m we find that $t[2^m - 1, 2^m - me - 1] = e + 1$, which tells us that BCH codes with $e > 2$ do not realize $t[n, k]$ for large n.

Furthermore, since

$$n - \lceil e \log n \rceil > n + 2 - \lceil (e+2) \log (n+2) \rceil,$$

we find that

$$\begin{aligned} t[n+2, n - \lceil e \log n \rceil] &\leq t[n+2, n+2 - \lceil (e+2) \log (n+2) \rceil] \\ &\leq e + 2 = t[n, n - \lceil e \log n \rceil] + 1. \end{aligned} \tag{35}$$

This result can be stated as

Proposition 14: For n large enough with respect to $n - k$, $t[n+2, k] \leq t[n, k] + 1$.

Corollary 6 (Corollary to Proposition 12): For all positive integers c and p, there are integers n, k such that

$$t[n, k] = t[n+1, k] = \cdots = t[n+c, k] = p.$$

In a similar vein, following an idea of Helleseth [22], we have the next proposition.

Proposition 15: For all c with $0 < c < 1/2$, there are n, k such that $t[n, k-1] > t[n, k] + 2^{ck}$.

Proof: If not, then there is a $c < 1/2$ such that for all n, k

$$t[n, k-1] \leq t[n, k] + 2^{ck}.$$

Iterating this inequality we get

$$t[n, k-2] \leq t[n, k] + 2^{ck} + 2^{c(k-1)},$$

and eventually

$$\lfloor n/2 \rfloor = t[n, 1] \leq t[n, k] + k2^{ck},$$

which contradicts (31).

VIII. Miscellaneous Results on Covering Radius

A. BCH Codes

Let us begin by summarizing what is known on the covering radii of the BCH codes of length $n = 2^m - 1$. Let BCH(e) denote the BCH code of packing radius e. BCH(1) is of course the Hamming code, with covering radius 1. BCH(2) has covering radius 3 [15], and BCH(3) has covering radius 5 [24], [19], [77]. The last result required considerable effort and, for the case $m = 4N + 2$, rested on the bound of Carlitz–Uchiyama [78], which in turn depended on the proof [57] by Weil of the Riemann hypothesis for function fields over finite fields of constants. More recently Helleseth [23] has used that bound to prove the following.

Theorem 16: $2e - 1 \leq t(\text{BCH}(e)) \leq 2e + 1$ for large m. This result also holds for nonprimitive BCH codes. Tietevainen [71] has improved the upper bound of this theorem to $2e$.

B. Recent Work of Helleseth

Here we summarize part of [23]. The problem of finding the covering radius of a binary cyclic code with irreducible generator polynomial is equivalent to Waring's problem in GF(2^m). Hence bounds on covering radius yield information on Waring's problem.

One can in principle use cyclotomic numbers to determine the covering radius and minimum distance in a cyclic code with irreducible generator polynomial over GF(q) for any q. There is Theorem 16, above, and a class of BCH(e) codes for which $t \geq 2e + 1$.

C. A Walsh-Transform Approach

In [26] the Walsh transform of the characteristic function h of the columns of the parity check matrix for C is used to formulate an algorithm for the calculation of $t(C)$. The number of additions required is at most $t(C)(n - k)2^{n-k}$, of multiplications $(t(C) - 1)2^{n-k}$, and of memory cells $3 \cdot 2^{n-k}$.

D. Results of Wolfmann and Assmus–Pless

These results explore the situation when the Delsarte bound is attained.

Theorem 17 [58]: If C is an $[n, k]$ code over GF(q), and $d_1, \cdots, d_N$ are the nonzero weights of vectors in $C^\perp$, then $t(C) = N$ implies that the number of coset leaders in any coset of weight $t(C)$ is constant, namely

$$(d_1 \cdots d_N)/N!q^{k-n}.$$

Theorem 17 was extended to the next theorem.

Theorem 18 [2]: Under the same hypotheses, the weight distribution of any coset of weight $t(C) = \text{N}$ is uniquely determined.

Theorem 18 also follows from [12, Theorem 3.2].

In the next result the hypothesis $t(C) = N$ is not used.

Theorem 19 [58]: Under the same notation, we find that $(d_1 \cdots d_N) \equiv 0 \pmod{t(C)!}$ and if $k \geq N$, the same congruence holds mod $t(C)!q^{k-N}$.

From Theorem 19 Wolfmann concludes that a doubly even [112, 56] self-dual code has at least 16 nonzero weights, and that the quadratic-residue code of type [14, 7, 6] over GF(4) has covering radius 3. (For the latter, the weights are 6, 8, 12, 14, the product of which is not 0 mod $4!4^3$.)

There are five mutually inequivalent extremal doubly even binary [32, 16, 8] self-dual codes, and all have covering radius 6 [2].

E. Nonbinary BCH Codes; Complexity

Nonbinary BCH Codes: Consider BCH codes over GF(q) of length $q^n - 1$, where q is a prime power.

Theorem 20 [55]: Let q be odd. Then the BCH code of designed distance at least 3 has covering radius

$$\begin{cases} 3 & \text{if } n \text{ is even or } q = 3 \\ 2 & \text{if } n \text{ is odd and } q > 3. \end{cases}$$

A formula for the number of coset leaders of each weight appears in [20].

Complexity: Starting from related work [7], McLoughlin has recently shown in [38] that the problem of finding the covering radius is not only *NP*-hard, but is even Π_2^ℓ-hard (in the terminology of [39]). By the latter term we mean that a problem that is complete for the class Π_2^ℓ is reducible to the covering radius problem. Thus to find the covering radius is strictly harder than any *NP*-complete problem unless the polynomial hierarchy collapses with $NP = \Pi_2^\ell$.

IX. Open Problems

1) Find $t(\text{RM}(1, 2s + 1))$. It is conjectured [42] that this quantity is asymptotic to $2^{2s} - 2^{(2s-1)/2}$, the upper bound in Section IV-A (re "Small Values of r").

2) For given n, k, which codes realize $t[n, k]$?

3) Define $K(n, \rho)$ as the minimum cardinality of any code, not necessarily linear, with length n and covering radius ρ. We know only a few values of $K(n, \rho)$. For example, when $\rho = 1$, $K(n, 1) = 2, 2, 4, 7, 12, 16, 32$ for $n = 2, 3, 4, 5, 6, 7, 8$. It would be interesting to find more values of $K(n, \rho)$. (See [64]–[70] and [79].)

4) Denote by $M(\Delta)$ the largest e such that there is a nontrivial linear binary code with covering radius t and packing radius e such that $t - e \leq \Delta$. Is it true that $M(\Delta) < \infty$ for all Δ? We know that $M(0) = 3$. The point of the question is whether $M(\Delta)$ remains finite for all infinite sequences of codes with lengths tending to infinity. By Theorem 14 we know it does so if the rate is bounded away from zero and one. For general $q \neq 2$ the only known fact is $M(0) < \infty$ [8].

5) Is it true that $t[n + 2, k] \leq t[n, k] + 1$ for all n, k? It is proved when the code has distance ≤ 3 (Lemma 2) or when n is large with respect to $n - k$ (35).

6) Determine the covering radii of some classes of codes (e.g., Goppa, Justesen, cyclic, quadratic residue, Reed–Muller).

7) For $K = 2^k$, is $t(n, K)$ always attained by linear codes?

8) For all n, k is there a code C realizing $t[n, k]$ with the all-one vector in C?

9) We know that for fixed k and large enough n,

$$n/2 - 8(k+1)^{1/2}(\log e)^{-1/2}2^{(k+1)/2} \le t[n,k] \le n/2 - 2^{(k-4)/2}.$$

Is it true that $t[n, k] \sim n/2 - C \cdot 2^{k/2}$ for some constant C, or that for constants C_1, C_2

$$C_1 < (n/2 - t[n,k])2^{-k/2} < C_2$$

for all large k?[1]

10) Among $[n, k]$ codes realizing $t[n, k]$, is there one with the all-one vector in a column of a parity check matrix H if H has the form $H = I_{n-k}; D$?

11) For $r \neq m - 1$, does the Reed–Muller code RM(r, m) have even covering radius? It does for $r = 0, 1$ (m even), $m - 3, m - 2, m$, and similarly for other extended cyclic codes.

12) For $m > m_0(e)$, prove $t(\mathrm{BCH}_e) = 2e - 1$ (conjectured in [23]).

13) Is $t\ [2s + 1, 4] = s - 2$?

14) What can be determined about the complexity of computing $t[n, k]$?

15) Is there a relation between the covering radius of a linear code and that of its orthogonal code? Is there a sort of MacWilliams relation for the coset spaces of the two codes?

Acknowledgment

The third-named author is grateful to l'École Nationale Superieure de Télécommunications for hospitality and support during the writing of this paper in the summer of 1983 and to Syracuse University for support in the same period.

We thank Peter Frankl for a helpful discussion, especially for calling our attention to [3] and [41]. We also thank A. Lobstein for contributions to Table II. We are grateful to the referees for their constructive comments, and we specially thank N. J. A. Sloane for close readings of drafts of this paper and for his many constructive and helpful suggestions.

We are grateful to Ms. Elaine Weinman for her capable typing and for her patience during many revisions of this work.

[1] 9) and 13) are answered in the affirmative in [72].

Appendix A
Nomenclature

C	A code.
$C^\perp$	Code orthogonal, or dual, to C when C is linear.
$d(C)$	Minimum Hamming distance of C.
$e(C)$	$= \lfloor (d(C) - 1)/2 \rfloor$, Packing radius of C.
$t(C)$	Covering radius of C.
$[n, k, d]$	Length, dimension, and $d(C)$ for linear code C.
(n, K, d)	Length, cardinality, and $d(C)$ for nonlinear code C.
$t[n, k]$	Minimum covering radius among all $[n, k]$ codes.
$t(n, K)$	Minimum covering radius among all nonlinear (n, K) codes.
$\Delta(C)$	$= t(C) - e(C)$.
$\mathrm{wt}(x)$ or $\lvert x \rvert$	Hamming weight of vector x or cardinality of x as support of vector.
$\mathbf{1}, \mathbf{0}$	All-1 or all-0 vector of length determined by context.
log	Logarithm to the base 2.
$H(x)$	$-x \log x - (1-x)\log(1-x)$.
I_m	$m \times m$ identity matrix.
$d(v, A) = \mathrm{wt}(v + A)$	Least Hamming distance from vector v to points of $A \subseteq Z_2^n$.
Z_2	Field of two elements.
Z_2^n	Set of all n-tuples over Z_2.
C_2/C_1	Set of *nonzero* coset leaders of C_2 mod C_1, one leader per coset.
$\subset$	Proper inclusion.

Appendix B

TABLE I
Some Codes of Known Covering Radius

Code C	Δ	n	k	$t(C)$	Reference
Repetition C_R	0	$2s+1$	1	s	
Hamming C_H	0	$2^m - 1$	$2^m - m - 1$	1	
Golay C_G	0	23	12	3	
Repetition C_R	1	$2s$	1	s	
Extended C_H	1	2^m	$2^m - m - 1$	2	
Extended C_G	1	24	12	4	
$C_H \times C_H$	1	$2(2^m - 1)$	$2(2^m - m - 1)$	2	
$C_H \times C_G$	1	$22 + 2^m$	$2^m - n + 11$	4	
Uniformly packed	1	$r(2^m - 1)$	$r(2^m - 1) - 2m$	2	
2-e.c. BCH	1	$2^m - 1$	$2^m - 2m - 1$	3	Section VIII-A
Punctured Preparata	1	$2^m - 1$	2^{n-2m+1}	3, m even, $m \ge 4$	
Zetterberg	1	$2^m + 1$	$n - 2m$	3, m even, $m \ge 4$	[74]
Red. Goppa	1	$2^m - 2$	$n - 2m$	3, m even, $m \ge 4$	[73]

TABLE I (*Continued*)

Code C	Δ	n	k	$t(C)$	Reference
Irred. Goppa	1	2^m	$n - 2m$	3, m odd	[74]
Melas	1	$2^m - 1$	$n - 2m$	3, m odd	[73]
Red. Goppa	2	$2^m - 2$	$n - 2m$	4, m odd	[73]
Irred. Goppa	2	2^m	$n - 2m$	4, m even	[74]
3-e.c. BCH	2	$2^m - 1$	$2^m - 3m - 1$	5	Section VIII-A
Quadratic residue	2	47	24	7	[12]
Doubly even, etc.	3	32	16	6	Section VIII-D
Geometry code	5	73	45	9	[46]
Simplex	2^{m-2}	$2^m - 1$	m	$2^{m-1} - 1$	[30, p. 173]
First-order Reed–Muller RM(1, m)	α	2^m	$m + 1$	$2^{m-1} - 2^{m/2-1}$, m even	Section V
RM($m - 3, m$)	$m + \delta - 3$	2^m	$2^m - 1 - m - \binom{m}{2} m + \delta$	$\delta = \begin{cases} 1, & m \text{ odd} \\ 2, & m \text{ even} \end{cases}$	Section V
	$\alpha = 2^{m-2} - 2^{(m-2)/2} - 1$				

TABLE II
VALUES AND BOUNDS ON $t[n, k]$ FOR $n \leq 32$ AND $k \leq 25$[a]

PART 1

k \ n	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
1	1	2	2	3	3	4	4	5	5	6	6	7	7	8	8	9	9	10	10
2	1	1	2	2	3	3	4	4	5	5	6	6	7	7	8	8	9	9	10
3	0	1	1	2	2	3	3	4	4	5	5	6	6	7	7	8	8	9	9
4		0	1	1	1	2	2	3	3	4	4	5	5	6	6	7	7–8	8	8–9
5			0	1	1	1	2	2	3	3	3–4	4	4–5	4–5	5–6	5–6	5–7	6–7	6–8
6				0	1	1	1	2	2	3	3	3	3–4	4–5	4–5	5	5–6	5–6	6
7					0	1	1	1	2	2	2–3	3	3	3–4	4	4–5	4–5	5	5–6
8						0	1	1	1	2	2	2	3	3	3–4	4	4–5	4–5	5
9							0	1	1	1	2	2	2	2–3	3	3–4	3–4	4–5	4–5
10								0	1	1	1	2	2	2	2–3	3	3	3–4	4
11									0	1	1	1	1	2	2	2–3	3	3	3–4
12										0	1	1	1	1	2	2	2–3	3	3
13											0	1	1	1	1	2	2	2–3	3
14												0	1	1	1	1	2	2	2
15													0	1	1	1	1	2	2
16														0	1	1	1	1	2
17															0	1	1	1	1
18																0	1	1	1
19																	0	1	1
20																		0	1
21																			0
22																			
23																			
24																			
25																			

[a] Here we present a table of values of and bounds on $t[n, k]$ for $n \leq 32$ and $k \leq 25$. The values for $k \leq 4$ were derived from the results in Section VI, and by a small computer search [79] for the values $t[15, 4]$, $t[17, 4]$, $t[16, 6]$, and $t[18, 6]$. The values for $k = 5$ come from the bound $t[2s + 1, 5] \leq t[2s, 4] = s - 2$, (see Proposition 11), from $t[2s, 5] \leq s - 3$, and from the sphere-covering lower bound in Section II-B. For $k = 6$ we use $t[n, 6] \leq t[n - 1, 5]$ and the lower bound in Section II-B. For $k > 6$ we use the upper bound $t[n + n', k + k'] \leq t[n, k] + t[n', k']$ and Lemma 2. Our most frequently used lower bound is from Section II-B.

An improved table of $t[n, k]$ appears in [72], where, in particular, $t[n, 4]$ and $t[n, 5]$ are determined for all n. Although we have seen that table, we have tried to exclude any of its new results from our table.

PART 2

k \ n	22	23	24	25	26	27	28	29	30	31	32
1	11	11	12	12	13	13	14	14	15	15	16
2	10	11	11	12	12	13	13	14	14	15	15
3	10	10	11	11	12	12	13	13	14	14	15
4	9	9–10	10	10–11	11	11–12	12	12–13	13	13–14	14
5	7–8	7–8	8–9	8–10	9–10	9–11	9–11	10–12	10–12	10–13	11–13
6	6–7	6–7	7–8	7–8	8–9	8–10	8–10	9–10	9–11	10–11	10–12
7	5–6	6–7	6–7	7–8	7–8	7–9	8–9	8–10	8–10	9–11	9–11
8	5–6	5–6	6–7	6–7	6–8	7–8	7–9	7–9	8–10	8–10	9–11

TABLE II, PART 2 (*Continued*)

k \ n	22	23	24	25	26	27	28	29	30	31	32
9	4–5	5–6	5–6	5–7	6–7	6–8	7–8	7–9	7–9	8–10	8–10
10	4–5	4–5	5–6	5–6	5–7	6–7	6–8	6–8	7–9	7–9	7–9
11	4	4–5	4–5	5–6	5–6	5–7	6–7	6–8	6–8	7–9	7–9
12	3	3	4	4	4–5	5–6	5–6	5–7	6–7	6–8	6–8
13	3	3	3	4	4	4–5	5	5–6	5–6	6–7	6–7
14	3	3	3	3	4	4	4–5	5	5–6	5–6	6–7
15	2	2–3	3	3	3	4	4	4–5	5	5	5–6
16	2	2	2–3	3	3	3	4	4	4	4–5	5
17	2	2	2	2–3	3	3	3	4	4	4	4–5
18	1	2	2	2	2–3	3	3	3	3–4	4	4
19	1	1	2	2	2	2–3	3	3	3	3–4	4
20	1	1	1	2	2	2	2–3	3	3	3	3–4
21	1	1	1	1	2	2	2	2–3	3	3	3
22	0	1	1	1	1	2	2	2	2	3	3
23		0	1	1	1	1	2	2	2	2	2–3
24			0	1	1	1	1	2	2	2	2
25				0	1	1	1	1	2	2	2

REFERENCES

[1] E. F. Assmus, Jr. and H. F. Mattson, Jr., "Coding and combinatorics," *SIAM Rev.*, vol. 16, pp. 349–388, 1974.

[2] E. F. Assmus, Jr. and V. Pless, "On the covering radius of extremal self-dual codes," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 359–363, 1983.

[3] J. Beck and T. Fiala, "'Integer-making' theorems," *Discrete Appl. Math.*, vol. 3, pp. 1–8, 1981.

[4] T. Berger, *Rate Distortion Theory*. Englewood Cliffs, NJ: Prentice-Hall, 1971.

[5] E. R. Berlekamp, *Algebraic Coding Theory*. New York: McGraw-Hill, 1968.

[6] E. Berlekamp and L. R. Welch, "Weight distributions of the cosets of the (32, 6) Reed–Muller code," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 203–207, 1972.

[7] E. R. Berlekamp, R. J. McEliece, and H. C. A. van Tilborg, "On the inherent intractability of certain coding problems," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 384–386, 1978.

[8] M. R. Best, "Perfect codes hardly exist," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 349–351, 1983.

[9] G. Cohen, "A nonconstructive upper bound on covering radius," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 352–353, 1983.

[10] G. Cohen and P. Frankl, "Good coverings of Hamming spaces with spheres," *Ann. Discrete Math.*, to appear.

[11] B. Courteau and J. Wolfmann, "Codes projectifs à deux ou trois poids et ensembles à sommes triples," *Discrete Math.*, to appear.

[12] P. Delsarte; "Four fundamental parameters of a code and their combinatorial significance," *Inform. Contr.*, vol. 23, pp. 407–438, 1973.

[13] I. I. Dumer and V. A. Zinovev, "Some new maximal codes over GF(4)," *Probl. Peredachi Inform.*, vol. 41, no. 3, pp. 24–34, July–Sep. 1978.

[14] G. David Forney, Jr., *Concatenated Codes*. Cambridge: Mass. Inst. Tech., 1966.

[15] D. Gorenstein, W. W. Peterson, and N. Zierler, "Two-error correcting Bose–Chaudhuri codes are quasi-perfect," *Inform. Contr.*, vol. 3, pp. 291–294, 1960.

[16] J. H. Griesmer, "A bound for error-correcting codes," *IBM J. Res. Develop.*, vol. 4, pp. 532–542, 1960.

[17] 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.

[18] T. Helleseth, T. Kløve, and J. Mykkeltveit, "On the covering radius of binary codes," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 627–628, 1978.

[19] T. Helleseth, "All binary 3-errors correcting BCH codes of length $2^m - 1$ have covering radius 5," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 257–258, 1978.

[20] ——, "The weight distribution of the coset leaders for some classes of codes with related parity-check matrices," *Discrete Math.*, vol. 28, pp. 161–171, 1979.

[21] ——, "No primitive binary t-error-correcting BCH-code with $t > 2$ is quasi-perfect," *IEEE Trans. Inform. Theory*, vol. IT-25, pp. 361–362, 1979.

[22] ——, private communication, Apr. 1981.

[23] ——, "Some analogies between algebraic and arithmetic codes," *Discrete Appl. Math.*, to appear.

[24] J. A. Van der Horst and T. Berger, "Complete decoding of triple-error-correcting binary BCH codes," *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 138–147, 1976.

[25] T. Kasami, "The weight enumerators for several classes of subcodes of the 2nd order binary Reed–Muller codes," *Inform. Contr.*, vol. 18, pp. 369–394, 1971.

[26] M. Karpovsky, "Weight distribution of translates, covering radius, and perfect codes...," *IEEE Trans. Inform. Theory*, vol. IT-27, pp. 462–472, 1981.

[27] A. Kotzig, personal communication.

[28] P. V. Kumar, R. A. Scholtz, and L. R. Welch, "Generalized bent functions and their properties," preprint.

[29] J. H. van Lint, *Coding Theory*. New York: Springer, 1971.

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

[31] H. F. Mattson, Jr., "An upper bound on covering radius," *Ann. Discrete Math.*, vol. 17, pp. 453–458, 1983.

[32] H. F. Mattson, Jr. and J. R. Schatz, "A brief survey of covering radius," *Ann. Discrete Math.*, vol. 18, pp. 617–624, 1983.

[33] H. F. Mattson, Jr., "Another upper bound on covering radius," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 356–359, 1983.

[34] T. Helleseth and H. F. Mattson, Jr., "On the cosets of the simplex code," preprint.

[35] R. J. McEliece, "Quadratic forms over finite fields and second-order Reed–Muller codes," *JPL Space Programs Summary*, Jet Propulsion Lab, Pasadena, CA, Rep. 37-58-III, pp. 28–33, 1973.

[36] A. McLoughlin, "On the covering radius," Ph.D. dissertation, Syracuse Univ., Syracuse, NY, 1977.

[37] ——, "The covering radius of the $(m-3)$rd order Reed–Muller codes and a lower bound on the $(m-4)$th order Reed–Muller codes," *SIAM J. Appl. Math.*, vol. 37, pp. 419–422, 1979.

[38] ——, "The complexity of computing the covering radius of a code," *IEEE Trans. Inform. Theory*, vol. IT-30, pp. 800–804, Nov. 1984.

[39] A. R. Meyer and L. J. Stockmeyer, "The equivalence problem for regular expressions with squaring requires exponential time," in *Proc. 13th Ann. Symp. Switching Automata Theory*, IEEE Computer Soc., 1972.

[40] J. Mykkeltveit, "The Covering radius of the (128, 8) Reed–Muller code is 56," *IEEE Trans. Inform. Theory*, vol. IT-26, pp. 359–362, 1980.

[41] J. E. Olson and J. Spencer, "Balancing families of sets," *J. Comb. Theory*, Series A 25, pp. 29–37, 1978.

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

[43] W. W. Peterson and E. J. Weldon, Jr., *Error-correcting Codes*, 2d

ed. Cambridge, MA: Mass. Inst. Tech., 1972.
[44] V. Pless and E. A. Prange, "Weight distribution of all cyclic codes... [of length] 31 over GF(2)," unpublished memorandum, Sept. 1962.
[45] E. Prange, "Some cyclic error-correcting codes with simple decoding algorithms," Air Force Cambridge Research Center, Bedford, MA, Apr. 1958.
[46] ——, "The use of coset equivalence in the analysis and decoding of group codes," Air Force Cambridge Research Center, Bedford, MA., June, 1959.
[47] I. S. Reed and G. Solomon, "Polynomial codes over certain finite fields," *J. SIAM*, vol. 8, pp. 300–304, 1960.
[48] J. R. Schatz, "On the coset leaders of Reed–Muller codes," Ph.D. dissertation, Syracuse Univ., Syracuse, NY 1979.
[49] ——, "The second order Reed–Muller code of length 64 has covering radius 18," *IEEE Trans. Inform. Theory*, vol. IT-27, pp. 529–530, 1981.
[50] ——, "On the weight distributions of cosets of a linear code," *Amer. Math. Mon.*, vol. 87, pp. 548–551, 1980.
[51] R. C. Singleton, "Maximum distance q-nary codes," *IEEE Trans. Inform. Theory*, vol. IT-10, pp. 116–118, 1964.
[52] N. J. A. Sloane and E. R. Berlekamp, "Weight-enumerator for second-order Reed–Muller codes," *IEEE Trans. Inform. Theory*, vol. IT-16, pp. 745–751, 1970.
[53] N. J. A. Sloane and R. J. Dick, "On the enumeration of cosets of first order Reed–Muller codes," in *Proc. IEEE Int. Conf. Communications*, vol. 7, 1971, pp. 36-2–36-6.
[54] H. C. A. van Tilborg, *Uniformly Packed Codes*. Eindhoven, The Netherlands: Eindhoven Tech. Univ., 1976.
[55] R. J. Turyn, "The covering radius of some BCH codes," in Sci. Rep. No. 1, *Research to Develop the Algebraic Theory of Codes*, Sylvania Applied Research Lab., Waltham, MA, June 1967.
[56] T. J. Wagner, "A search technique for quasi-perfect codes," *Inform. Contr.*, vol. 9, pp. 94–99, 1966.
[57] A. Weil, "On the Riemann hypothesis in function-fields," *Proc. NAS*, vol. 27, pp. 345–347, 1941.
[58] J. Wolfmann, "Résultats sur les paramètres des codes linéaires," *Revue du Cethedec*, pp. 25–33, 1979.
[59] ——, "Un probleme d'extremum dans les espaces vectoriels binaires," *Ann. Discrete Math.*, vol. 9, pp. 261–264, 1980.
[60] ——, "Une construction de codes projectifs à deux poids," Revue du Cethedec, no. 66, pp. 77–84, 1981.
[61] J. H. Conway, R. A. Parker, and N. J. A. Sloane, "The covering radius of the Leech lattice," in *Proc. Royal Soc.*, London, 1982, vol. A380, pp. 261–290.
[62] J. H. Conway and N. J. A. Sloane, "Voronoi regions of lattices, second moments of polytopes, and quantization," *IEEE Trans. Inform. Theory*, vol. IT-28, pp. 211–226, 1982.
[63] ——, "Fast quantizing and decoding algorithms for lattice quantizers and codes," *IEEE Trans. Inform. Theory*, vol. IT-28, pp. 227–232, 1982.
[64] J. G. Kalbfleisch and R. G. Stanton, "A combinatorial problem in matching," *J. London Math. Soc.*, vol. 44, pp. 60–64, 1969.
[65] J. G. Kalbfleisch, R. G. Stanton, and J. D. Horton, "On covering sets and error-correcting codes," *J. Comb. Theory*, vol. 11A, pp. 233–250, 1971.
[66] J. G. Kalbfleisch and P. H. Weiland, "Some new results for the covering problem," in *Recent Progress in Combinatorics*. New York: Academic, 1969, pp. 37–45.
[67] H. J. L. Kamps and J. H. van Lint, "The football pool problem for 5 matches," *J. Comb. Theory*, vol. 3, pp. 315–325, 1967.
[68] ——, "A covering problem," in *Combinatorial Theory and its Applications*, P. Erdös, A. Rényi, and V. T. Sós, Eds. Amsterdam: North-Holland, 1970, pp. 679–685.
[69] R. G. Stanton and J. G. Kalbfleisch, "Covering problems for dichotomized matchings, *Aequationes Math.*, vol. 1, pp. 94–103, 1968.
[70] ——, "Intersection inequalities for the covering problem," *SIAM J. Appl. Math.*, vol. 17, pp. 1311–1316, 1969.
[71] A. Tietevainen, personal communication to T. Helleseth, 1983.
[72] R. L. Graham and N. J. A. Sloane, "On the covering radius of codes," *IEEE Trans. Inform. Theory*, this issue.
[73] O. Moreno, "Further results on quasiperfect codes related to the Goppa codes," *Congressus Numerandium*, vol. 40, pp. 249–256, 1983.
[74] ——, "Quasiperfect double error correcting codes," *IEEE Trans. Inform. Theory*, to appear.
[75] O. Rothaus, "On 'bent' functions," *J. Comb. Theory*, vol. 20, pp. 300–305, 1976.
[76] J. F. Dillon, "Elementary Hadamard difference sets," Ph.D. thesis, Univ. Maryland, College Park, 1974.
[77] ——, "Some 3-error correcting BCH codes have covering radius 5," *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 348–349, 1976.
[78] L. Carlitz and S. Uchiyama, "Bounds for exponential sums," *Duke Math J.*, vol. 24, pp. 37–41, 1957.
[79] A. Lobstein, thèse de troisième cycle, to appear.
[80] L. B. Levitin and C. R. P. Hartmann, "The zero-neighbors algorithm," *IEEE Trans. Inform. Theory*, this issue.