© DISCRETE MATHEMATICS 3 (1972) 265–294. North-Holland Publishing Company

A SURVEY OF CONSTRUCTIVE CODING THEORY, AND A TABLE OF BINARY CODES OF HIGHEST KNOWN RATE

N.J.A. SLOANE

Bell Telephone Laboratories, Inc., Murray Hill, N.J., U.S.A.

Received 6 November 1971

Abstract. Although more than twenty years have passed since the appearance of Shannon's papers, a still unsolved problem of coding theory is to construct block codes which attain a low probability of error at rates close to capacity. However, for moderate block lengths many good codes are known, the best-known being the BCH codes discovered in 1959. This paper is a survey of results in coding theory obtained since the appearance of Berlekamp's "Algebraic coding theory" (1968), concentrating on those which lead to the construction of new codes. The paper concludes with a table giving the smallest redundancy of any binary code, linear or nonlinear, that is presently known (to the author), for all lengths up to 512 and all minimum distances up to 30.

§1. Introduction

This paper is a survey of recent developments in the design of block codes for the correction of random errors.

In 1948, Shannon [98] showed that there exist codes which attain a low probability of error at rates close to capacity. Gilbert [31] in 1952 obtained a lower bound on d/n for the best codes of a given rate. Since then a great deal of effort has been made to construct arbitrarily long codes which meet or even come close to the Gilbert bound, but so far without success (except for codes with rates approaching 0 or 1).

For moderate block lengths, however, many good codes have been discovered. The best-known are the Reed–Muller (RM) codes ([79], [93], [B1, Ch. 15]), Bose–Chaudhuri–Hocquenghem (BCH) codes ([19], [45], [B1, Ch. 7 and Ch. 10]), and quadratic residue (QR) codes ([B1, Ch. 15], [111, §4.4]). A systematic description of these and other codes discovered prior to 1968 will be found in [B1].

In this paper we describe some of the developments in coding theory

that have taken place since the appearance of [B1]. We concentrate on those papers which construct new codes, or give new properties of codes previously known. Important topics not considered here are the weight enumeration of codes [7, 8, 10, 14, 15, 32, 41, 53–57, 73, 81, 86, 94, 100, 106, 114], the classification of cosets of a code [9, 16, 94, 103], decoding techniques and burst error correction [20, 85, 95, 109, 110], synchronization recovery [105], and source coding and rate distortion theory [6, 47]. See also the recent survey of Goethals [35], which is of broader scope than the present work, and the book by Van Lint [111]. We have had little access to Russian work, and refer the reader to the surveys by Kautz and Levitt [58] and Dobrushin [30].

The paper is arranged as follows. §2 deals with cyclic and related codes, including BCH, irreducible, perfect, abelian group, Goppa Srivastava, and circulant codes. §3 deals with nonlinear codes and codes formed by combining other codes. §4 gives a table containing the best binary codes known to the author. An extensive bibliography concludes the paper. A shortened preliminary version of this paper has appeared in [102].

§2. Cyclic codes

Most of the codes considered to date have been linear and cyclic, for the excellent reasons that such codes are simpler to implement and to analyze.

An (n, k) *linear code* $\mathcal{C}$ over the field GF(q) consists of q^k vectors (called *codewords*) of length n over GF(q) such that (a) the sum, taken componentwise in GF(q), of any two codewords is again a codeword, and (b) the componentwise product of any codeword and any element of GF(q) is also a codeword. The *redundancy* of the code is $r = n - k$ and the *rate* is $R = k/n$. The *minimum distance* is denoted by d.

The *dual* code $\mathcal{C}^\perp$ of $\mathcal{C}$ consists of all vectors u of length n over GF(q) such that $u \cdot v = 0$ for all $v \in \mathcal{C}$, the scalar product being evaluated in GF(q). Thus $\mathcal{C}^\perp$ is an $(n, n-k)$ linear code. If $\mathcal{C} = \mathcal{C}^\perp$, $\mathcal{C}$ is *self-dual*.

An application of self-dual codes to a famous unsolved problem of geometry is given in [74].

A code is *shortened* by omitting all codewords except those having

prescribed values for certain components, and then deleting those components [B1, p. 336].

A *cyclic code* is a linear code with the property that a cyclic shift of any codeword is also a codeword. BCH, QR, and shortened RM codes are all cyclic.

2.1. *Are long cyclic codes bad?* Gilbert [31] showed that there exist arbitrarily long linear codes with a fixed rate $R = k/n$ for which d/n is bounded away from zero. In fact Koshelev [59] and Kozlov [60] have shown that most linear codes meet the Gilbert bound.

On the other hand for BCH codes of fixed rate R, $d/n \to 0$ as $n \to \infty$ ([67], [B1, Ch. 12]). In fact Berlekamp [12] has recently shown that for BCH codes

$$d \sim \frac{2n \ln R^{-1}}{\log n}$$

as $n \to \infty$. But it is not known whether long cyclic codes are also bad.

Berman [18] has shown that cyclic codes of fixed rate and with block lengths n which are divisible by a fixed set of primes (and only by these primes) have bounded minimum distance.

Kasami [52] has shown that good linear codes cannot be too symmetric, by showing that any code with given d/n which is invariant under the affine group must have rate $R \to 0$ as $n \to \infty$. (This includes BCH codes.)

More recently McEliece [77] showed that it is not the symmetry alone that makes a code bad, by showing that there exist arbitrarily long block codes (not necessarily linear) which are invariant under large permutation groups and which meet the Gilbert bound. Also Weldon [23], [118] has shown that there exist very, but not arbitrarily, long circulant and quasi-cyclic codes which meet the Gilbert bound. (A quasi-cyclic code is a linear code with the property that a cyclic shift of any codeword by a certain prescribed number of places is also a codeword. Circulant codes are defined in §2.9.) Weldon's proof would apply to arbitrarily long codes if the conjecture were proved that there are an infinite number of primes for which 2 is a primitive root.

Kasami [52] and Chen [22] have shown that there exist arbitrarily long shortened cyclic codes which meet the Gilbert bound.

Thompson (see [75]) has shown that self-dual linear binary codes in which all weights are divisible by 4 meet the Gilbert bound.

To give a rough summary of these results, a good family of codes can be linear, or have many symmetries, but not both.

2.2. BCH *codes*. We recall the definition of a BCH code. Let q be a prime power, let m be the order of q modulo n, and let α be a primitive n^{th} root of unity in GF(q^m). Then the BCH *code* of length n, designed distance $d = d_{\text{BCH}}$, and symbols from GF(q), has the parity check matrix

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{2(n-1)} \\ \vdots & & & & \vdots \\ 1 & \alpha^{d-1} & \alpha^{2(d-1)} & \dots & \alpha^{(n-1)(d-1)} \end{pmatrix}.$$

If $n = q^m - 1$ the code is called *primitive*. By the BCH bound any such code has actual minimum distance

$$d_{\min} \geq d_{\text{BCH}}.$$

It was conjectured [55], [B1, p. 295] that for primitive BCH codes $d_{\min} = d_{\text{BCH}}$, but in 1969 Kasami and Tokura [K2] showed that for $m > 6$, $m \neq 8, 12$, there are binary primitive BCH codes of length $n = 2^m - 1$ for which

$$d_{\min} > d_{\text{BCH}}.$$

On the other hand Berlekamp [8] showed that if the extended binary BCH code of length $n = 2^m$ has $d_{\text{BCH}} = 2^{m-1} - 2^i$ for some $i \geq \frac{1}{2}m - 1$, then $d_{\min} = d_{\text{BCH}}$. The results of [8] have been further generalized by Kasami [53]. But the precise determination of conditions on n and d_{BCH} for $d_{\min} = d_{\text{BCH}}$ to hold remains an unsolved problem.

Leont'ev [66] showed that a BCH code of length $n = 2^m - 1$ and designed distance $2t + 1$ is not quasi-perfect for $2 < t < \sqrt{n}/\ln n$ and $m \geq 7$.

V.M. Sidel'nikov [100] showed that for $t < \sqrt{n}/10$, the number of words of weight w in the binary BCH code of designed distance $2t + 1$ is $(n+1)^{-t}\binom{n}{w}(1 + \epsilon)$, where $|\epsilon| < Cn^{-0.1}$, for most values of w.

Anderson ([1], [111, p. 127]) obtained the following bound for the dual of a BCH code, using deep number-theoretic results of Weil, Carlitz and Uchiyama. The minimum distance of the dual of the binary BCH code of length $n = 2^m - 1$ and designed distance $d_{\mathrm{BCH}} = 2t+1$ is at least

$$2^{m-1} - 1 - (t-1)^{\frac{1}{2}m} .$$

2.3. *Extensions of* BCH *codes.* Wolf [117] showed that two columns may be added to the parity check matrix of a BCH code to give the new parity check matrix

$$H' = \begin{pmatrix} 1 & 0 & \\ 0 & 0 & \\ \dots & & H \\ 0 & 1 & \end{pmatrix},$$

while preserving the minimum distance of the code. In some cases the redundancy is also unchanged, in which case we have a new code with

$$n' = n+2, \quad k' = k+2, \quad r' = r, \quad d' = d .$$

This happens for example when the original code is a Reed–Solomon code over GF(q), with $n = q-1$ and $r = d-1$. Then the parameters of the new code are $n' = q+1$, and $r' = d' - 1 = d-1$.

It is easy to show that for any code $d \leq r+1$. Codes with $d = r+1$ are called *maximum distance separable* or MDS codes (see [101], [B1, p. 309], [111, p. 72]). Such codes have also been called *optimal*. Reed–Solomon codes are MDS and so are the new family of doubly extended Reed–Solomon codes.

Assmus and Mattson [3] have shown that MDS codes whose block length n is a prime number are very common, by showing that every cyclic code of prime length n over GF(p^i) is MDS, for all i, for all except a finite number of primes p.

Wolf [118] has obtained a further extension of BCH codes, by replacing α in H' by the $m \times m$ matrix A over GF(q), where

$$A = \begin{pmatrix} 0 & 1 & 0 & & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & 0 & 0 & & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ a_0 & a_1 & a_2 & & a_{m-1} \end{pmatrix}$$

and where $M(x) = x^m - a_{m-1}x^{m-1} - \ldots - a_0$ is the minimal polynomial of α over GF(q). Call the new parity check matrix H''. Then if H generates a primitive BCH code over GF(q) of length $n = q^m - 1$, designed distance d_{BCH} and redundancy $r = m(d_{\text{BCH}} - 1)$, so that this is a maximally redundant BCH code, then H'' is the parity check matrix for a code over GF(q) with $n' = m(q^m + 1)$, $r = m(d_{\text{BCH}} - 1)$ and $d \geq d_{\text{BCH}}$. The rate of the code has thus been considerably increased.

For example, if the original code is over GF(5) with $n = 5^2 - 1 = 24$, $d_{\text{BCH}} = 5$, $k = 16$, $R = 0.67$, the new code has $n = 52$, $k = 44$, $d \geq 5$ and $R = 0.87$.

Other extensions of BCH codes are mentioned in §3.3.

2.4. *The minimum distance of cyclic codes.* The BCH bound for a cyclic code says that if the generator polynomial $g(x)$ has $d_{\text{BCH}} - 1$ consecutive roots then the minimum distance is $\geq d_{\text{BCH}}$.

Goethals [33] and Kasami [51] have given improvements on the BCH bound for codes of composite length. Hartmann [38–43] has given many further generalizations of the BCH bound, including extensions of Kasami's results. We will just state two of Hartmann's theorems. Here β denotes a primitive n^{th} root of unity. The first is a bound on the minimum odd weight.

Theorem. *Let $k|n$. If for some $\bar{d} \leq n/k$, $g(\beta^{ki}) = 0$ for all $i = 1, 2, \ldots, \bar{d}$, then the minimum odd weight is at least $\bar{d}$.*

Example. By the BCH bound the (33, 13) BCH code has $d_{\text{BCH}} = 5$, and also $d_{\text{even}} \geq 10$. But by the theorem $d_{\text{odd}} \geq 11$, and so the minimum weight is ≥ 10.

The second theorem is an example of Hartmann's generalizations of the BCH bound to the case where $g(x)$ has several sets of consecutive roots.

Theorem. *If* $g(\beta^{m_0+i+\delta(j-1)}) = 0$ *for* $i = 0, 1, 2, \ldots, d-1$ *and* $j = 1, 2, \ldots, r$ *with* $(\delta, n) = 1$, *so that* $g(x)$ *has* r *sets of* $d-1$ *roots each, then* $d_{\min} \geq d + r$.

Kasami and Tokura [K2] have shown that for any even $m \geq 6$ there exist binary cyclic codes of length $2^m - 1$ having more codewords than the corresponding BCH codes. The first such example is a (63, 28) $d = 15$ cyclic code, compared with the (63, 24) $d = 15$ BCH code.

Chen [C3] used an IBM 360/50 to calculate the minimum distance of all binary cyclic codes of lengths ≤ 65. He found three codes of length 63 having more codewords than the corresponding BCH codes. These are the (63, 28) code just mentioned, a (63, 46) $d = 7$ code given previously by Peterson [86], and a (63, 21) $d = 18$ code. The BCH codes closest to the last two are (63, 45) $d = 7$ and (63, 18) $d = 21$ codes.

2.5. *Irreducible cyclic codes.* A cyclic code over GF(q) is called irreducible if its check polynomial $h(x)$ is irreducible over GF(q) [111, p. 45]. The simplest examples of irreducible codes are maximal length shift register $(2^m - 1, m)$ codes (also known as shortened first order RM codes).

Baumert, McEliece, and Rumsey [5], [78], generalizing earlier work of Delsarte and Goethals [29], have given a method for finding the weight enumerators of all irreducible cyclic codes. For example in the binary case, let N be a fixed odd number and let k be the smallest positive number such that $2^k \equiv 1 \pmod N$. Then there are binary irreducible cyclic $(n = (2^{km} - 1)/N, km)$ codes $\mathcal{C}_m$, for $m = 2, 3, \ldots$. Each $\mathcal{C}_m$ consists of the zero vector plus N cycles of n codewords each. Let $w_0, w_1, \ldots, w_{N-1}$ be the weights of these cycles. Then the generating function $w_0 + w_1 y + \ldots + w_{N-1} y^{N-1}$ is given by

$$2^{m-1}(E(y))^m \pmod{y^N - 1}$$

where $E(y)$ is independent of m. For example when $N = 7$ we obtain (9, 6), (73, 9), (585, 12), (4681, 15), ... codes with minimum distances

respectively equal to 2, 28, 280, 2320, ... (The complete weight distributions are given in [78].)

The weight distributions of several other families of cyclic codes have been given by Oganesyan and Yagdzhan [81], [92]. We just mention one of these, which consists of codes with check polynomials of the form $h(x) = \prod_{i=0}^{f} p_i(x)$, where $p_0(x)$ is irreducible of degree k_0 and period e_0, $m_0 = (2^{k_0}-1)/e_0$ is prime, 2 is a primitive root of m_0, $p_i(x)$ is a primitive polynomial of degree k_i and period e_i, and the numbers e_i are relatively prime.

2.6. *Perfect codes.* An e-error-correcting code over GF(q) is called *perfect* if every vector is at a distance of at most e from the nearest codeword.

Examples of perfect codes are various trivial codes containing 1, 2, or q^n codewords; the Hamming $d = 3$ codes over any field; and the two Golay codes, the (11, 6) $d = 5$ code over GF(3) and the (23, 12) $d = 7$ code over GF(2).

A long-standing conjecture that no other perfect codes exist over finite fields has recently been proved by Tietäväinen, using earlier work of Lloyd and Van Lint [107], [108], [112].

The (12, 6) and (24, 12) extended Golay codes have many important combinatorial properties. Their symmetry groups are the Mathieu groups M_{12} and M_{24}; their low weight vectors form the Steiner systems $S(5, 6, 12)$ and $S(5, 8, 24)$; and the lattices Λ_{12} and Λ_{24} (the Leech lattice) can be constructed from them [62], [65]. A series of uniqueness theorems have been proved: Pless [87] showed the uniqueness of the Golay codes, Stanton [104] the uniqueness of the Mathieu groups, Witt [116] the uniqueness of the associated Steiner systems, and Conway [24], [25] the uniqueness of the Leech lattice.

Goethals [34] showed that the Nordstrom–Robinson code (§3.2) is contained in the (24, 12) code. Berlekamp [11] has studied the symmetry groups of the principal subcodes of the (24, 12) code.

Since the Nordstrom–Robinson code is the first member of Preparata's family of nonlinear double-error correcting codes (§3.2), it is natural to ask if the others can be extended to give codes analogous to the Golay code. However, Preparata [91] has shown that this is impossible, in one way at least.

Turyn [2] showed that the (24, 12) Golay code may be obtained as the set of vectors of the form $(a+x, b+x, a+b+x)$ $a, b \in \mathcal{C}_1$, $x \in \mathcal{C}_2$, where $\mathcal{C}_1$ and $\mathcal{C}_2$ are two different first order RM codes. The same construction was used in [S4] to obtain an infinite family of linear codes with $d/n = \frac{1}{3}$. The first three codes of the family are the (24, 12) Golay code, and (48, 15) $d = 16$ and (96, 18) $d = 32$ codes. As the length increases the rate approaches zero. A generalization of the (12, 6) Golay code is described in the next section.

Parker and Nikolai [82] described an unsuccessful search for simple transitive groups analogous to the Mathieu groups.

2.7. *Abelian group codes.* Let $\mathcal{C}$ be a binary cyclic (n, k) code. If codewords are represented by polynomials, $c_0 c_1 \ldots c_{n-1} \leftrightarrow c_0 + c_1 x + \ldots + c_{n-1} x^{n-1}$, then it is well known that the codewords in $\mathcal{C}$ form an ideal in the ring of polynomials modulo $x^n - 1$ [P1, Ch. 8].

MacWilliams [71], [72], Berman [17], [18] and others [21], [27] have studied the following generalization of cyclic codes. Let $G = \{g_1, \ldots, g_n\}$ be a multiplicative abelian group, and let R denote the set of all formal sums

$$c_1 g_1 + c_2 g_2 + \ldots + c_n g_n, \; c_i = 0 \text{ or } 1$$

with the obvious addition and multiplication. R is a vector space of dimension n over GF(2). An ideal $\mathcal{A}$ is a linear subspace of R such that if $A \in \mathcal{A}$, $g \in G$ then $gA \in \mathcal{A}$. Then $\mathcal{A}$ is a natural generalization of a cyclic code, and is called an abelian group code.

Many properties of cyclic codes carry over to abelian group codes, such as the existence of a generator codeword whose multiples generate the code.

Berman [18] has shown that for fixed rate and for block lengths n which are divisible by a fixed set of primes (and only by these primes), as $n \to \infty$ abelian group codes have higher minimum distance than cyclic codes.

2.8. *Goppa and Srivastava codes.* Goppa [G4] has recently described a new family of linear noncyclic codes, some of which meet the Gilbert bound.

Let integers m, t be given satisfying $3 \leq m < mt < 2^m$. Let

$$Z = \{z \in \mathrm{GF}(2^{mt}) \mid \text{degree of minimal polynomial of } z \text{ is } mt\},$$

and let α be a primitive element of $\mathrm{GF}(2^m)$. Then for any $z \in Z$ the binary Goppa code $\mathcal{G}(m, t, z)$ is the $(n = 2^m, k \geq 2^m - mt)$ code with the $mt \times 2^m$ parity check matrix

$$H = \left[\frac{1}{z-0}, \frac{1}{z-1}, \frac{1}{z-\alpha}, \ldots, \frac{1}{z-\alpha^{2^m-2}}\right].$$

Goppa has shown that the minimum distance of $\mathcal{G}(m, t, z)$ is (i) at least $2t+1$ for all $z \in Z$, (ii) equal to that given by the Gilbert bound for some $z \in Z$. Unfortunately it is not known how to choose $z \in Z$ so as to make this happen.

Srivastava codes [B1, § 15.1] resemble Goppa codes. Helgert [H2], [H3] has recently found a number of good Srivastava codes.

2.9. *Circulant codes.* In 1964 Leech [61] showed that the generator matrix for the (23, 12) Golay code can be written as

$$\left[\begin{array}{ccc|ccc} 1 & & & & C & \\ & \ddots & & & & \\ & & 1 & 1 & \ldots & 1 \end{array}\right]$$

where C is a circulant matrix, that is, each row is a cyclic shift of the previous row by one place. In this case the first row of C can be taken to be 1 1 0 1 1 1 0 0 0 1 0, having a 1 at position 0 and at the quadratic residues of 11.

Then in 1965 in an important paper ([K1], see also [46], [49], [50]) Karlin found a large number of binary codes generated by circulants, many having a higher rate than the best codes previously known. Examples are (27, 14), (30, 16), (34, 12), and (53, 14) codes, having minimum distances respectively equal to 7, 7, 11 and 17.

This approach also simplified the calculation of the minimum distance, and Karlin was able to determine the minimum distance of a number of

binary quadratic residue codes, e.g., the (79, 40) $d = 15$ and (89, 45) $d = 17$ QR codes. Karlin also asserts that the QR codes of lengths 103 and 107 both have minimum distance equal to 19.

Pless [88], [89] has constructed self-dual $(2q+2, q+1)$ codes over GF(3) for every odd prime power $q \equiv -1 \pmod 3$. These are circulant codes, with a generator matrix of the form

$$\left[\begin{array}{cccc|cccc} 1 & & & & 1 & & & \\ & 1 & & & 1 & & C & \\ & & 1 & & 1 & & & \\ & & & 1 & 0 & 1 & 1 & 1 \end{array}\right]$$

where C is a circulant matrix. The first five are (12, 6) (the ternary Golay code), (24, 12), (36, 18), (48, 24) and (60, 30) codes, with minimum distances 6, 9, 12, 15 and 18 respectively. These five codes have rate $\frac{1}{2}$ and $d = \frac{1}{4}n + 3$. But unfortunately later codes in the family have smaller distances. Nevertheless circulant codes are a very promising area for research.

§3. Nonlinear codes and codes formed by combining other codes

Since the number of codewords in a nonlinear code need not be a power of the alphabet size, it is convenient to have a new notation:

An (n, M, d) code $\mathcal{C}$ is a set of M codewords of length n, with symbols from GF(q) and minimum distance d. The dimension of this code is $k = \log_q M$, the redundancy is $r = n - \log_q M$, and the rate is $R = k/n$. Now k and r need not be integers.

A *coset* of $\mathcal{C}$ is an arbitrary translation $a + \mathcal{C}$ of the codewords of $\mathcal{C}$ (where a is any vector of length n). If $\mathcal{C}$ is linear, then two cosets of $\mathcal{C}$ are either equal or disjoint, but this need not be true if $\mathcal{C}$ is nonlinear.

An (n, M, d) code is said to be *optimal* if it has the largest possible number of codewords for the given values of n and d. This is using optimal in a very naive sense, of course, since it omits any consideration of encoding and decoding. But it can be argued that once good codes have been found, the techniques for their implementation will be developed later, as has happened with BCH codes [B1, Ch. 7].

It seems reasonable to expect that optimal codes will often be nonlinear, and that even near-optimal linear codes will have a complicated structure. As a well-known verse by J.L. Massey [70] says, "... good codes just might be messy."

Nonlinear codes have been successfully used to construct dense sphere packings in Euclidean space [63–65].

3.1. *Codes derived from Hadamard and conference matrices.* An $n \times n$ *Hadamard matrix* $\mathcal{H}_n$ is a matrix of +1's and −1's such that $\mathcal{H}_n \mathcal{H}_n^t = nI$ (where I is a unit matrix). Replacing +1's by 0's and −1's by 1's converts $\mathcal{H}_n$ into a *binary Hadamard* matrix H_n.

It was shown by Plotkin [P1, p. 79], [P3], [B1, p. 316] that the $(n, 2n, \frac{1}{2}n)$ code consisting of the rows of H_n and its complement is optimal. When n is a power of 2 this is a (linear) first order Reed–Muller code, while in the other cases this is a nonlinear Hadamard code.

Many other nonlinear codes can be obtained by manipulating Hadamard matrices. Levenshtein ([L2], see also [58, p. 206], [83]) showed that optimal codes for all d and all $n \leq 2d$ can be obtained in this way (provided the requisite Hadamard matrices exist) by showing that such codes meet the Plotkin bound [P3]. Patel [84] has determined the optimal linear codes in the same region.

Recently [S2] good nonlinear codes with n slightly greater than $2d$ have been obtained from conference matrices. An $n \times n$ *conference matrix* T_n is a matrix with 0's on the diagonal and ±1's elsewhere, satisfying $T_n T_n' = (n-1)I$. Whenever a symmetric T_n exists, an $(n-1, 2n, \frac{1}{2}(n-2))$ binary nonlinear code can be constructed. The first few codes obtained are the (9, 20, 4) optimal code of Julin [J1], a (13, 28, 6) code which is inferior to Nadler's code [80], the (17, 36, 8) code given in [S1], and (25, 52, 12), (29, 60, 14), (37, 76, 18), (41, 84, 20) codes.

3.2. *Preparata and Kerdock codes.* Nonlinear double-error-correcting codes were constructed by Nadler ([80], a (12, 32, 5) code), Green ([37], (13, 64, 5)), and Nordström and Robinson ([N1], $(15, 2^8, 5)$). Van Lint [114] has given a simple construction of the Nadler code.

Preparata [P4] gave a high-rate generalization of the Nordström–Robinson code. For every even $m \geq 4$ he constructed a nonlinear $(2^m - 1, 2^{2^m - 2m}, 5)$ code. These codes are optimal, contain twice as many code-

words as double-error-correcting BCH codes, and have straightforward encoding and decoding algorithms.

Semakov and Zinov'ev [96], [97] and Goethals and Snover [36] have independently obtained the weight distribution of the Preparata codes.

Kerdock [K5] has given a corresponding low-rate generalization of the Nordström–Robinson code. He showed that for every even $m \geq 4$ it is possible to take the union of the $(2^m, 2^{m+1}, 2^{m-1})$ first order RM code and $2^{m-1}-1$ of its cosets to obtain a

$$(2^m, 2^{2m}, 2^{m-1}-2^{\frac{1}{2}(m-2)})$$

nonlinear code. For $m = 4$ this is the extended Nordström–Robinson code; for $m = 6$ this is a $(64, 2^{12}, 28)$ code containing four times as many codewords as the best extended cyclic code of that length and distance.

The Preparata and Kerdock codes are "duals" in the sense that their weight distributions satisfy the MacWilliams identity [B1, p. 401]. The reason for this is not yet understood.

The next four sections describe constructions for combining two, three, or four codes to obtain new codes.

3.3. *Constructions X and X4.* Construction X combines three codes to form a fourth. Suppose we are given an (n_1, M_1, d_1) code $\mathcal{C}_1$ and an $(n_1, M_2 = bM_1, d_2)$ code $\mathcal{C}_2$, with the property that $\mathcal{C}_2$ is the union of b disjoint cosets of $\mathcal{C}_1$,

$$\mathcal{C}_2 = (x_1 + \mathcal{C}_1) \cup (x_2 + \mathcal{C}_1) \cup \ldots \cup (x_b + \mathcal{C}_1),$$

for some set of vectors $S = \{x_1, x_2, \ldots, x_b\}$. Let

$$\mathcal{C}_3 = \{y_1, y_2, \ldots, y_b\}$$

be any (n_3, b, Δ) code.

Let π be an arbitrary permutation of $\{1, 2, \ldots, b\}$; so that $x_i \to y_{\pi(i)}$ defines a one-one mapping from S onto $\mathcal{C}_3$.

The new code is then defined to be

$$\mathcal{C}_4 = (x_1 + \mathcal{C}_1, y_{\pi(1)}) \cup (x_2 + \mathcal{C}_1, y_{\pi(2)}) \cup \ldots$$

$$\ldots \cup (x_b + \mathcal{C}_1, y_{\pi(b)}) .$$

Simply stated, $\mathcal{C}_2$ is divided into cosets of $\mathcal{C}_1$, and a different codeword of $\mathcal{C}_3$ is attached to each coset. See fig. 1.

Then $\mathcal{C}_4$ is an $(n_1 + n_3, M_2, d = \min\{d_1, d_2 + \Delta\})$ code. Similarly construction $X4$ combines four codes to form a fifth. See [S4] for details and further examples.

Example 1. Take $\mathcal{C}_1$ to be a Preparata code, $\mathcal{C}_2$ a Hamming code, $\mathcal{C}_3$ an even weight code. Then, after showing that the Hamming code is a union of cosets of the Preparata code, one obtains $(2^m + m - 1, 2^{2^m - m - 1}, 5)$ codes for $m \geq 4$. Using construction $X4$ one can do even better, and extend the Preparata code by the addition of $\sqrt{n+1}$ information symbols at the cost of adding one check symbol [S4].

Example 2. Using BCH codes one obtains new codes having at least as many codewords as those given by the Andryanov–Saskovets construction [B1, p. 333]. In some cases e-error-correcting BCH codes may be extended by the addition of about $n^{1/e}$ information symbols at the cost of adding one check symbol [S4].

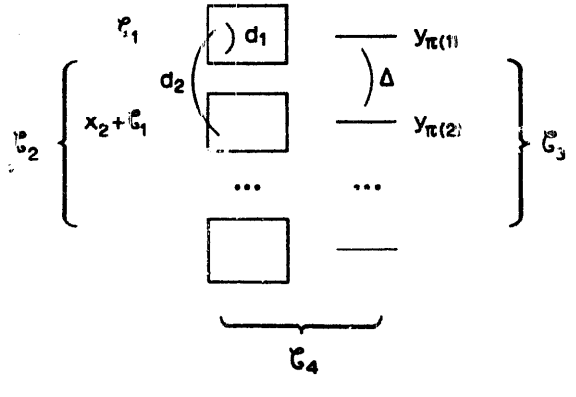

Fig. 1.

3.4. *Constructions* $Y1$, $Y2$, $Y3$. The following constructions were suggested by Goethals [34].

Construction $Y1$. Let $\mathcal{C}_1$ be an $(n, 2^{k_1}, d_1)$ linear code and let $\mathcal{C}_2$ be its $(n, 2^{r_1}, d_2)$ dual code, with coordinates chosen so that there is a minimum weight codeword $1 \ldots 10 \ldots 0$ in $\mathcal{C}_2$. Let S be the subgroup of $\mathcal{C}_1$ in which the first $d_2 - 1$ coordinates are zero. Then the d_2^{th} coordinates of S are also zero. If the initial d_2 zeros are deleted from S we are left with an

$$(n - d_2, 2^{k_1 - d_2 + 1}, d_1)$$

linear code.

Construction $Y2$. Let T be the union of S and all of the $d_2 - 1$ cosets of S in $\mathcal{C}_1$ with coset leaders $110^{n-2}, 1010^{n-3}, \ldots, 10^{d_2-2}10^{n-d_2}$. By deleting the first d_2 coordinates of T we obtain an

$$(n - d_2, d_2 2^{k_1 - d_2 + 1}, d_1 - 2)$$

nonlinear code.

Construction $Y3$. Taking all the cosets with coset leaders of weight 2 we obtain an

$$\left(n - d_2, \left(1 + \binom{d_2}{2}\right) 2^{k_1 - d_2 + 1}, d_1 - 4\right)$$

nonlinear code.

Many examples of codes obtained by these constructions are given in [S4].

3.5. *Construction Z.* This combines two codes to form a third [P3], [44], [S1], [68].

Let $\mathcal{C}_1 = (n_1, M_1, d_1)$ and $\mathcal{C}_2 = (n_2, M_2, d_2)$ be arbitrary codes over GF(q). Let o denote the zero vector of length $|n_1 - n_2|$. Then the new code $\mathcal{C}_3$ is defined as follows.

(i). If $n_1 \leq n_2$, $\mathcal{C}_3 = \{(x, (x, o) + y) \mid x \in \mathcal{C}_1, y \in \mathcal{C}_2\}$, and is an

$(n_1 + n_2, M_1M_2, d = \min(2d_1, d_2))$ code. (In the definition of $\mathcal{C}_3$, the comma denotes concatenation and + denotes vector addition in GF(q).)

(ii). If $n_1 > n_2$, $\mathcal{C}_3 = \{(x, x + (y, 0)) \mid x \in \mathcal{C}_1, y \in \mathcal{C}_2\}$, and is a $(2n_1, M_1M_2, d = \min(2d_1, d_2))$ code.

$\mathcal{C}_3$ is linear if $\mathcal{C}_1$ and $\mathcal{C}_2$ are. A number of applications are given in [S1], including the construction of an infinite family of nonlinear single-error-correcting codes which contain more codewords than shortened Hamming codes. Other examples, of which those in table 1 are typical, will be seen in table 2.

3.6. *Assmus and Mattson's rate $\frac{1}{3}$ cyclic codes.* Let p be a prime of the form $8N+5$ for which 2 is a primitive root (e.g., $p = 5, 13, 29, 37, \ldots$). Assmus and Mattson [4] showed how to concatenate three different versions of the $(p, p-1)$ even weight code to obtain a linear binary cyclic $(3p, p-1)$ code, denoted by $3E$, with minimum distance at least $2\sqrt{3p}$. Let $3E^+$ be the cyclic $(3p, p)$ code consisting of the codewords of $3E$ together with their complements. The first few examples of $3E^+$ are (15, 5) $d = 7$, (39, 13) $d = 12$, (87, 29) $d = 24$, and (111, 37) $d = 24$ codes.

3.7. *Other constructions.* Other techniques for constructing codes have been given in [26], [28], [76], [99]. However the codes obtained appear to contain fewer, or at best as many, codewords as known cyclic codes.

Table 1

$\mathcal{C}_1$			$\mathcal{C}_2$			$\mathcal{C}_3$		
n_1	r_1	d_1	n_2	r_2	d_2	n	r	d
23	11	7	11	4.830	4	34	15.830	7
19	12	8	19	18	19	38	30	16
14	13	14	264	101	27	278	114	27

§4. A table of the best codes presently known

4.1. For a given value of the length n and minimum distance d, let M be the maximum number of codewords of any binary (n, M, d) code, linear or nonlinear, that is presently known (to the author). Then table 2 gives the redundancy $r = n - \log_2 M$ of this code as a function of n and d, for all $n \leq 512$ and $d \leq 30$. These codes are of considerable theoretical interest in themselves, provide a basis for judging new codes, and as a lower bound to the densest possible codes complement Johnson's table of upper bounds [48]. Previous tables of codes are to be found in [B1], [C1], [C3], [G3], [L1], [P1], [P3], [W1], and [86].

4.2. *Types of codes.* The codes are classified as follows.

B = Bose–Chaudhuri–Hocquenghem code [B1, Ch. 7].
C = Cyclic linear code [P1, Ch. 8].
D = Goppa code ([G4] and §2.8 above).
G = Group or linear code [P1, Ch. 3].
H = Hadamard code [L2].
J = Code from conference matrix [S2].
K = Circulant code [K1].
N = Nonlinear code.
P = Nordström–Robinson–Preparata code [N1], [P4].
Q = Quadratic residue code ([B1, §15.2], [111, §4.4]).
R = Reed–Muller code [B1, §15.3].
S = Srivastava code [B1, §15.1], [H2].
XA, XC, XP = Codes from construction X applied to BCH codes (the generalized Andryanov–Saskovets construction), to cyclic codes, and to Preparata codes respectively ([S4] and §3.3 above).
X4 = Codes from construction $X4$ ([S4] and §3.3 above).
Y1, Y2, Y3 = Codes from constructions $Y1$, $Y2$, $Y3$ ([S4] and §3.4 above).
Z = Codes from construction Z ([S1] and §3.5 above).

Types B, C, D, G, K, Q, R, S, XA, XC, Y1 are linear, H, J, N, P, XP, Y2, Y3 are nonlinear, and X4, Z may be linear or nonlinear.

In table 2, codes for which the reference [S3] is given are new. With one exception these are all examples of constructions mentioned in the

text. The exception is an (85, 18) $d = 25$ which was obtained using construction 39 of Hatcher [44].

4.3. Since an $(n, M, d$ odd) code is equivalent to an $(n+1, M, d+1)$ code, only codes for odd d need be given. An (n, M, d) code may be punctured to give $(n-i, M, d-i)$ codes for $0 < i < d$, or shortened to give $(n-i, M2^{-i}, d)$ codes for $0 < i < \log_2 M$. In table 2 all such modified codes carry the name of the original code. An (n, M, d) of redundancy r may be thought of as an $(n+i, M, d)$ code of redundancy $r+i$, for $i \geq 1$, in which case the name is left blank.

4.4. Some nonlinear codes in table 2 have redundancy r which is not a whole number. In such cases the number of codewords is quickly found as follows: If $r = R + a$, where R is a whole number and $0 < a < 1$, the number of codewords is $M = i2^{n-R-5}$ where i is given by

a	.046	.093	.142	.193	.245	.300	.356	.415	.541	.608	.678	.752	.830	.913
i	31	30	29	28	27	26	25	24	22	21	20	19	18	17

4.5. In many cases the reference is to a place where the complete weight distribution of the code may be found, rather than to the original determination of the minimum distance.

4.6. Although many of these codes may be optimal, in the sense of having the smallest possible redundancy, very few of them are known to be optimal. (Compare [48].) The reader is invited to try and improve on them. Those of type Z and distances 25–29 are especially weak. The author is eager to hear of any improvements.

4.7. In the first section of table 2, for minimum distance $d = 3$, when $n = 3, 4, 5$ and $3 \cdot 2^{m-2} \leq n < 2^m$, $m \geq 3$, the codes shown are (shortened) Hamming codes [H1]. When $2^m \leq n < 3 \cdot 2^{m-1}$, $m \geq 3$, the codes shown are nongroup codes, discovered by Golay [G2] and Julin [J1] for $n = 8, 9, 10, 11$ and by Sloane and Whitehead [S1] for $n \geq 16$.

Acknowledgments

I should like to thank H.L. Berger for his help in collecting data for table 2, E.R. Berlekamp for information about recent Russian work, F.J. MacWilliams for helpful comments on the manuscript, and H.J. Helgert for supplying a number of good codes.

Table 2
Binary codes of length n, minimum distance d, and smallest known redundancy r

Distance $d = 3$ (see sect. 4.7 in this paper)	
n	r
4– 7	3
8	3.678
9	3.752
10– 11	3.830
12– 15	4
16– 17	4.678
18– 19	4.752
20– 23	4.830
24– 31	5
32– 35	5.678
36– 39	5.752
40– 47	5.830
48– 63	6
64– 71	6.678
72– 79	6.752
80– 95	6.830
96–127	7
128–143	7.678
144–159	7.752
160–191	7.830
192–255	8
256–287	8.678
288–319	8.752
320–383	8.830
384–511	9
512	9.678

Distance $d = 5$			
n	r	Type	Ref.
7– 8	6	G	[L1]
9– 11	6.415	H	[P3]
12– 15	7	P	[N1]
16– 19	8	XP	[S4]
20	8.678	X4	[S4]
21– 23	9	G	[W1]
24– 32	10	B	[G3]
33– 63	11	P	[P4]
64– 70	12	X4	[S4]
71– 73	13	S	[H2]
74–128	14	B	[S4]
129–255	15	P	[P4]
256–271	16	X4	[S4]
272–277	17	S	[H2]
278–512	18	B	[S4]

Distance $d = 7$			
n	r	Type	Ref.
10– 11	9	G	[L1]
12– 15	10	R	[P1]
16	10.830	J	[S1]
17– 23	11	Q	[G1]
24	12		
25– 27	13	K	[K1]
28– 30	14	K	[K1]
31– 32	15	D	[G4]
33	15.752	Z	[S3]
34– 35	15.830	Z	[S3]
36– 47	16	G*	
48– 63	17	C	[C3]
64– 67	18	XC	[S4]
68– 70	19	XA	[S3]
71– 83	20	S	[H2]
84–128	21	D	[G4]
129–135	22	XA	[S3]
136–159	23	Y1	[S4]
160–256	24	D	[G4]
257–264	25	XA	[S3]
265–311	26	S	[H2]
312–512	27	D	[G4]

* From S.M. Reddy

Table 2 (continued)

Distance $d = 9$

n	r	Type	Ref.
13– 14	12	G	[L1]
15	13		
16	13.415	H	[L2]
17– 19	13.678	H	[L2]
20	14.678		
21	15.415	H	[L2]
22	16.300	J	[S2]
23– 25	16.678	Y2	[S4]
26	17.678		
27– 29	18	B	[P1]
30– 35	18.415	Y2	[S4]
36	19.415		
37– 41	20	Q	[B1]
42– 45	21	Q	[P2]
46	22		
47– 49	22.193	Y2	[S4]
50– 52	23	S	[H2]
53– 73	24	B	[K3]
74– 75	25–26		
76– 90	27	S	[H2]
91–128	28	B	[S4]
129–135	29	XA	[S3]
136	30		
137–156	31	S	[H2]
157–256	32	B	[S4]
257–264	33	XA	[S3]
265	34		
266–311	35	S	[H3]
312–512	36	B	[S4]

Distance $d = 11$

n	r	Type	Ref.
16– 17	15	G	[L1]
18	16		
19	16.415	H	[L2]
20	17	B	[G3]
21– 23	17.415	H	[L2]
24	18.300	J	[S2]
25– 26	19	G	[H3]
27– 31	20	B	[P1]
32	21		
33– 35	22	Y1	[S4]
36– 47	23	Q	[P2]
48– 50	24–26		
51– 63	27	B	[P1]
64– 67	28	XA	[S3]
68– 70	29–31		
71– 74	32	XC	[S4]
75	33		
76– 94	34	S	[H3]
95–128	35	D	[G4]
129–135	36	XA	[S3]
136–137	37–38		
138–156	39	S	[H3]
157–256	40	D	[G4]
257–264	41	XA	[S3]
265–266	42–43		
267–311	44	S	[H3]
312–512	45	D	[G4]

Table 2 (continued)

Distance $d = 13$				Distance $d = 15$			
n	r	Type	Ref.	n	r	Type	Ref.
19– 20	18	G	[C2]	22– 23	21	G	[C2]
21– 22	19–20			24– 25	22–23		
23	20.415	H	[L2]	26	23.415	H	[L2]
24	21	G	[C1]	27	24	G	[L2]
25– 27	21.193	H	[L2]	28	24.678	H	[L2]
28	22.093	J	[S2]	29– 31	25	R	[P1]
29	23	R	[P1]	32	26		
30	24			33	26.830	H	[L2]
31	24.830	H	[L2]	34	27.752	J	[S2]
32	25.752	J	[S2]	35	28	Z	[S3]
33– 37	26	XA	[S3]	36– 37	29	Z	[S3]
38	27			38– 41	30	XC	[S4]
39– 43	28	C	[B1]	42	31		
44– 45	29–30			43– 47	32	G	[S4]
46– 55	31	Y2	[S4]	48– 50	33	C	[B1]
56	32			51– 55	34	C	[B1]
57– 63	33	B	[P1]	56– 63	35	C	[K2]
64– 70	34	XA	[S3]	64– 66	36	XC	[S4]
71– 72	35–36			67– 68	37–38		
73– 77	37	Q	[K1]	69– 71	38.830	Y2	[S4]
78– 79	38–39			72– 79	39	Q	[K1]
80– 85	40	Q	[K1]	80– 81	40–41		
86– 96	41	S	[H3]	82– 87	42	Q	[K1]
97–128	42	B	[S4]	88– 91	43–46		
129–135	43	XA	[S3]	92– 99	47	Q	[K1]
136–138	44–46			100	48		
139–156	47	S	[H3]	101–128	49	D	[G4]
157–256	48	B	[S4]	129–135	50	XA	[S3]
257–264	49	XA	[S3]	136–140	51–55		
265–267	50–52			141–256	56	D	[G4]
268–311	53	S	[H3]	257–264	57	XA	[S3]
312–512	54	B	[S4]	265–269	58–62		
				270–512	63	D	[G4]

Table 2 (continued)

Distance $d = 17$

n	r	Type	Ref.
25– 26	24	G	[C2]
27– 28	25–26		
29	26.415	H	[L2]
30	27.415		
31	28	G	[L2]
32	28.415	H	[L2]
33– 36	28.830	H	[L2]
37	29.752	J	[S2]
38	30.678	H	[L2]
39	32.541	H	[L2]
40	33.541		
41	34	N	[H3]
42	35	G	[H3]
43– 46	36	G	[H3]
47– 49	37	G	[K4]
50	38		
51– 53	39	K	[K1]
54– 55	39	Y3	[S4]
56	40	Y1	[S4]
57– 62	41	C	[C3]
63– 66	42	XC	[S4]
67– 71	43	Y1	[S4]
72– 89	44	Q	[K1]
90– 93	45–48		
94–101	49	Q	[K1]
102	50		
103–105	51	K	[K1]
106–107	52–53		
108–125	54	B	[P1]
126	55		
127–128	56	B	[S4]
129–135	57	XA	[S3]
136–141	58–63		
142–256	64	B	[S4]
257–264	65	XA	[S3]
265–270	66–71		
271–512	72	B	[S4]

Distance $d = 19$

n	r	Type	Ref.
28– 29	27	G	[C2]
30– 32	28–30		
33	30.415	H	[L2]
34	31	C	[C3]
35	31.678	H	[L2]
36	32.415	H	[L2]
37– 39	32.678	H	[L2]
40	33.608	J	[S2]
41	34.541	H	[L2]
42	35.541		
43	36.415	H	[L2]
44	37	G	[H3]
45– 48	38	G	[H3]
49– 51	39	G	[K4]
52– 54	40–42		
55– 61	43	B	[P1]
56– 57	42	Y3	[S4]
58– 61	43	B	[P2]
62– 63	44	C	[C3]
64	45		
65– 66	46	XC	[S4]
67– 68	47	XC	[S4]
69– 70	48	XC	[S4]
71– 74	49	XC	[S4]
75– 83	50	Y1	[S4]
84–103	51	Q	[K1]
104	52		
105–107	53	K	[K1]
108–109	54–55		
110–127	56	B	[P1]
128–131	57–60		
132–139	61	XC	[S4]
140–145	62–67		
146–255	68	B	[P1]
256–260	69	XA	[S3]
261–268	70–77		
269–270	78	Z	[S3]
271–272	79–80		
273–512	81	D	[G4]

Table 2 (continued)

Distance $d = 21$

n	r	Type	Ref.
31– 32	30	G	[C2]
33– 35	31–33		
36	33.415	H	[L2]
37	34.415		
38	35	G	[L2]
39	35.678	H	[L2]
40	36.193	H	[L2]
41– 43	36.541	H	[L2]
44	37.541		
45	38.415	H	[L2]
46	39.356	J	[S2]
47– 48	40	C	[C3]
49– 51	41–43		
52– 57	43.415	Y2	[S4]
58	44.415		
59– 63	45	B	[P1]
64– 70	46–52		
71– 77	53	XC	[S4]
78	54		
79– 85	55	K	[K1]
86– 92	56–62		
93–127	63	B	[P1]
128–135	64	XA	[S3]
136–144	65–73		
145–146	74	Z	[S3]
147	75		
148–255	76	B	[P1]
256–264	77	XA	[S3]
265–273	78–86		
274–275	87	Z	[S3]
276–277	88–89		
278–512	90	B	[S4]

Distance $d = 23$

n	r	Type	Ref.
34– 35	33	G	[C2]
36– 38	34–36		
39	36.415	H	[L2]
40	37.415		
41	38	G	[L2]
42	39		
43	39.415	H	[L2]
44	40	C	[C3]
45– 47	40.415	H	[L2]
48	41.356	J	[S2]
49– 50	42	C	[C3]
51– 53	43–45		
54– 57	46	Y1	[S4]
58– 63	47	B	[P1]
64– 66	48	XA	[S3]
67– 74	49–56		
75– 87	57	K	[K1]
88– 99	58–69		
100–127	70	B	[P1]
128–135	71	XA	[S3]
136–145	72–81		
146–147	82	Z	[S3]
148	83		
149–255	84	B	[P1]
256–264	85	XA	[S3]
265–274	86–95		
275–276	96	Z	[S3]
277–278	97–98		
279–512	99	D	[G4]

Table 2 (continued)

Distance $d = 25$

n	r	Type	Ref.
37– 38	36	G	[C2]
39– 42	37–40		
43	40.415	H	[L2]
44	41.415		
45	42	G	[L2]
46	42.678	H	[L2]
47	43.415	H	[L2]
48	44	G	[L2]
49– 51	44.300	H	[L2]
52	45.245	J	[S2]
53	46.193	H	[L2]
54	47.193		
55	48.093	H	[L2]
56– 61	49	N	[K5]
62– 63	50–51		
64– 66	52	K	[K1]
67	53		
68– 70	54	XA	[S3]
71	55		
72– 73	56	XC	[S4]
74– 83	57–66		
84– 85	67	G	[S3]
86– 88	68–70		
89	70.678	Z	[S3]
90	71.415	Z	[S3]
91	72	Z	[S3]
92– 94	72.300	Z	[S3]
95	73.245	Z	[S3]
96	74.193	Z	[S3]
97–125	75	B	[P1]
126–127	76–77		
128–135	78	XA	[S3]
136–146	79–89		
147–148	90	Z	[S3]
149	91		
150–255	92	B	[P1]
256–264	93	XA	[S3]
265–275	94–104		
276–277	105	Z	[S3]
278–279	106–107		
280–512	108	B	[S4]

Distance $d = 27$

n	r	Type	Ref.
40– 41	39	G	[C2]
42– 45	40–43		
46	43.415	H	[L2]
47	44.415		
48	45	C	[C3]
49	46		
50	46.678	H	[L2]
51	47.193	H	[L2]
52	47.830	H	[L2]
53– 55	48.193	H	[L2]
56	49.193		
57	50.093	H	[L2]
58– 63	51	N	[K5]
64– 69	52–57		
70– 74	58	XC	[S4]
75– 86	59–70		
87– 88	71	Z	[S3]
89	72		
90– 91	73	G	[S4]
92– 94	74–76		
95–127	77	B	[P1]
128–131	78–81		
132–139	82	XC	[S4]
140–150	83–93		
151–160	94	K	[K4]
161–165	95–99		
166–255	100	B	[P1]
256–264	101	XA	[S3]
265–276	102–113		
277–278	114	Z	[S3]
279–280	115–116		
281–512	117	D	[G4]

Table 2 (continued)

Distance $d = 29$

n	r	Type	Ref.
43– 44	42	G	[C2]
45– 48	43–46		
49	46.415	H	[L2]
50	47.415		
51	48.415		
52	49	G	[L2]
53	49.678	H	[L2]
54	50.415	H	[L2]
55	51.193	H	[L2]
56	51.678	H	[L2]
57– 59	52.093	H	[L2]
60	53.046	J	[S2]
61	54	R	[P1]
62	55		
63	55.913	H	[L2]
64	56.913		
65– 67	57	XA	[S3]
68– 74	58–64		
75– 78	65	XC	[S4]
79– 86	66–73		
87– 88	74	Z	[S3]
89– 93	75	G	[S4]
94– 97	76–79		
98	79.415	Z	[S3]
99–100	80.415	Z	[S3]
101	81.415		
102–125	82	B	[K2]
126–127	83–84		
128–135	85	XA	[S3]
136–148	86–98		
149–150	99	Z	[S3]
151–155	100–104		
156–158	105	Z	[S3]
159–160	106–107		
161–255	108	B	[P1]
256–264	109	XA	[S3]
265–277	110–122		
278–279	123	Z	[S3]
280–281	124–125		
282–512	126	B	[S4]

References

Abbreviations: BSTJ = Bell System Technical Journal, IC = Information and Control, JCT = Journal of Combinatorial Theory, PGIT = IEEE Transactions on Information Theory.

1. *References for the table of codes*

[B1] E.R. Berlekamp, Algebraic coding theory (McGraw-Hill, New York, 1968) (see especially pp. 360, 432–433).

[C1] L. Calabi and E. Myrvaagnes, On the minimal weight of binary group codes, PGIT 10 (1964) 385–387.

[C2] J.T. Cordaro and T.J. Wagner, Optimum (n, 2) codes for small values of channel error probability, PGIT 13 (1967) 349–350.

[C3] C.L. Chen, Computer results on the minimum distance of some binary cyclic codes, PGIT 16 (1970) 359–360.

[F1] A.B. Fontaine and W.W. Peterson, Group code equivalence and optimum codes, PGIT 5 (1959) (Special Suppl.) 60–70.

[G1] M.J.E. Golay, Notes on digital coding, Proc. IRE, 37 (1949) 657.

[G2] M.J.E. Golay, Binary coding, PGIT 4 (1954) 23–28.

[G3] H.D. Goldman, M. Kliman and H. Smola, The weight structure of some Bose–Chaudhuri codes, PGIT 14 (1968) 167–169.

[G4] V.D. Goppa, A new class of linear error-correcting codes, Prob. Peredači Inform. 6 (1970) 24–30 (in Russian).

[H1] R.W. Hamming, Error detecting and error correcting codes, BSTJ 29 (1950) 147–160.

[H2] H.J. Helgert, Srivastava codes, PGIT 18 (1972) 292–297.

[H3] H.J. Helgert, personal communication.

[J1] D. Julin, Two improved block codes, PGIT 11 (1965) 459.

[K1] M. Karlin, New binary coding results by circulants, PGIT 15 (1969) 81–92.

[K2] T. Kasami and N. Tokura, Some remarks on BCH bounds and minimum weights of binary primitive BCH codes, PGIT 15 (1969) 408–413.

[K3] T. Kasami, S. Lin and W.W. Peterson, Polynomial codes, PGIT 14 (1968) 807–814.

[K5] A.M. Kerdock, A class of low-rate nonlinear codes, IC 20 (1972) 182–187.

[K4] M. Karlin, personal communication.

[L1] A.E. Laemmel, Efficiency of noise reducing codes, in: W. Jackson, ed., Communication theory (Butterworth, London, 1953) 111–118.

[L2] V.I. Levenshtein, The application of Hadamard matrices to a problem in coding, Problems of Cybernetics 5 (1964) 166–184.

[L3] V. Lum and K.T. Chien, On the minimum distance of Bose–Chaudhuri–Hocquenghem codes, SIAM J. Appl. Math. 16 (1968) 1325–1337.

[N1] A.W. Nordstrom and J.P. Robinson, An optimum nonlinear code, IC 11 (1967) 613–616.

[P1] W.W. Peterson, Error-correcting codes (M.I.T. Press, Cambridge, Mass., 1961) (see especially pp. 71, 166–167).

[P2] V.S. Pless, Power moment identities on weight distributions in error correcting codes, IC 6 (1963) 147–152.

[P3] M. Plotkin, Binary codes with specified minimum distance, PGIT 6 (1960) 445–450.

[P4] F.P. Preparata, A class of optimum nonlinear double-error correcting codes, IC 13 (1968) 378–400.

[S1] N.J.A. Sloane and D.S. Whitehead, A new family of single-error correcting codes, PGIT 16 (1970) 717–719.

[S2] N.J.A. Sloane and J.J. Seidel, A new family of nonlinear codes obtained from conference matrices, Ann. New York Acad. Sci. 175 (1970) 363–365.
[S3] A new code.
[S4] N.J.A. Sloane, S.M. Reddy and C.L. Chen, New binary codes, PGIT 18 (1972) 503–510.
[T1] N. Tokura, K. Taniguchi and T. Kasami, A search procedure for finding optimum group codes for the binary symmetric channel, PGIT 13 (1967) 587–594.
[W1] T.J. Wagner, A search technique for quasi-perfect codes, IC 9 (1966) 94–99.

2. *Further references cited in text*

[1] D.R. Anderson, A new class of cyclic codes, SIAM J. Appl. Math. 16 (1968) 181–197.
[2] E.F. Assmus Jr., H.F. Mattson Jr. and R.J. Turyn, Research to develop the algebraic theory of codes (Sci. Rept. AFCRL-67-0365, Air Force Cambridge Res. Lab., Bedford, Mass., 1967).
[3] E.F. Assmus Jr. and H.F. Mattson Jr., New 5-designs, JCT 6 (1969) 122–151.
[4] E.F. Assmus Jr. and H.F. Mattson Jr., Some $(3p, p)$ codes, in: Information processing 68 (North-Holland, Amsterdam, 1969) 205–209.
[5] L.D. Baumert and R.J. McEliece, Weights of irreducible cyclic codes, to appear.
[6] T. Berger, Rate distortion theory (Prentice-Hall, Englewood Cliffs, N.J., 1971).
[7] E.R. Berlekamp, Weight enumeration theorems, in: Proc. 6th Allerton Conf. on Circuit and Systems Theory, Urbana (Univ. of Illinois Press, Chicago, Ill. 1968) 161–170.
[8] E.R. Berlekamp, The weight enumerators for certain subcodes of the second order binary Reed–Muller codes, IC 17 (1970) 485–500.
[9] E.R. Berlekamp, Some mathematical properties of a scheme for reducing the bandwidth of motion pictures by Hadamard smearing, BSTJ 49 (1970) 969–986.
[10] E.R. Berlekamp, A survey of coding theory for algebraists and combinatorialists (Intern. Centre for Mech. Sci., Udine, Italy, 1970).
[11] E.R. Berlekamp, Coding theory and the Mathieu groups, IC 18 (1971) 40–64.
[12] E.R. Berlekamp, Long primitive binary BCH codes have distance $d \sim 2n \ln R^{-1}/\log n$ ..., PGIT 18 (1972) 415–426.
[14] E.R. Berlekamp and N.J.A. Sloane, Weight enumerator for second order Reed–Muller codes, PGIT 16 (1970) 745–751.
[15] E.R. Berlekamp and L.R. Welch, Weight distributions of the cosets of the (32, 6) Reed–Muller code, PGIT 18 (1972) 203–207.
[16] E.R. Berlekamp, F.J. MacWilliams and N.J.A. Sloane, Gleason's theorem on self dual codes, 18 (1972) 409–414.
[17] S.D. Berman, On the theory of group codes, Cybernetics 3 (1967) 25–31.
[18] S.D. Berman, Semisimple cyclic and abelian codes II, Cybernetics 3 (1967) 17–23.
[19] R.C. Bose and D.K. Ray-Chaudhuri, On a class of error correcting binary group codes, IC 3 (1960) 68–79, 279–290.
[20] H.O. Burton, A survey of error correcting techniques for data on telephone facilities, in: Proc. Intern. Commun. Conf., San Francisco, Calif., 1970.
[21] P. Camion, Abelian codes, Math. Res. Center, Univ. of Wisconsin, Rept. 1059 (1970).
[22] C.L. Chen, The existence of arbitrarily long pseudo-cyclic codes that meet the Gilbert bound, in: Proc. 5th Ann. Princeton Conf. Inform. Sci. (1971) 242.
[23] C.L. Chen, W.W. Peterson and E.J. Weldon Jr., Some results on quasicyclic codes, IC 15 (1969) 407–423.
[24] J.H. Conway, A group of order 8,315,553,613,086,720,000, Bull. London Math. Soc. 1 (1969) 79–88.
[25] J.H. Conway, A characterization of Leech's lattice, Invent. Math. 7 (1969) 137–142.
[26] G. Dagnino, On a new class of binary group codes, Calcolo 5 (1968) 277–294.

[27] P. Delsarte, Automorphisms of abelian codes, Philips Res. Rept. 25 (1970) 389–402.
[28] P. Delsarte, Majority logic decodable codes derived from finite inversive planes, IC 18 (1971) 319–325.
[29] P. Delsarte and J.M. Goethals, Irreducible binary cyclic codes of even dimension, Univ. North Carolina at Chapel Hill, Inst. Statist., Mimeo Ser. No. 600.27, 1970.
[30] R.L. Dobrushin, Survey of Soviet research in information theory, to appear.
[31] E.N. Gilbert, A comparison of signaling alphabets, BSTJ 31 (1952) 504–522.
[32] A.M. Gleason, Weight polynomials of self-dual codes and the MacWilliams identities, in: Proc. Intern. Congr. Mathematicians, Nice (1970) 140–144.
[33] J.M. Goethals, Factorization of cyclic codes, PGIT 13 (1967) 242–246.
[34] J.M. Goethals, On the Golay perfect binary code, ICT 11 (1971) 178–186.
[35] J.M. Goethals, Some combinatorial aspects of coding theory, in: Proc. Combinat. Symp., Fort Collins, 1971, to appear.
[36] J.M. Goethals and S.L. Snover, Nearly perfect binary codes, Discrete Math. 3 (1972) 65–88 (this issue).
[37] M.V. Green Two heuristic techniques for block-code construction (Abstract), PGIT 12 (1966) 273.
[38] C.R.P. Hartmann, On the minimum distance structure of cyclic codes and decoding beyond the BCH bound, Ph. D. Thesis, Univ. of Illinois, 1970; also Coord. Sci. Lab. Rept. R-458, Univ. of Illinois, 1970.
[39] C.R.P. Hartmann, A note on the minimum distance structure of cyclic codes, PGIT 18 (1972) 439–440.
[40] C.R.P. Hartmann, A generalization of the BCH bound, submitted to IC.
[41] C.R.P. Hartmann, On the weight structure of cyclic codes of composite length, in: Proc. Fourth Hawaii Inter. Conf. System Sci., (1971) 117–119.
[42] C.R.P. Hartmann and K.K. Tzeng, A bound for cyclic codes of composite length, PGIT 18 (1972) 307.
[43] C.R.P. Hartmann, K.K. Tzeng and R.T. Chien, Some results on the minimum distance structure of cyclic codes, PGIT 18 (1972) 402–409.
[44] T. Hatcher, On minimal distance, shortest length, and greatest number of elements for binary group codes (Parke Mathematical Labs., Carlisle, Mass., Tech. Memo. 6, 1964).
[45] A. Hocquenghem, Codes correcteurs d'erreurs, Chiffres, 2 (1959) 147–156.
[46] C.W. Hoffner II and S.M. Reddy, Circulant bases for cyclic codes, PGIT 16 (1970) 511–512.
[47] F. Jelinek, Free encoding of memoryless time-discrete sources with a fidelity criterion, PGIT 15 (1969) 584–590.
[48] S.M. Johnson, On upper bounds for unrestricted binary error-correcting codes, PGIT 17 (1971) 466–478.
[49] M. Karlin, Decoding of circulant codes, PGIT 16 (1970) 797–802.
[50] M. Karlin, Weight/moment relationships in $(Q + E)$ circulants, unpublished.
[51] T. Kasami, Some lower bounds on the minimum weight of cyclic codes of composite length, PGIT 14 (1968) 814–818.
[52] T. Kasami, An upper bound on k/n for affine-invariant codes with fixed d/n, PGIT 15 (1969) 174–176.
[53] T. Kasami, The weight enumerators for several classes of subcodes of the second order binary Reed–Muller codes, IC 18 (1971) 369–394.
[54] T. Kasami, Some results on the weight structure of Reed–Muller codes, to appear.
[55] T. Kasami, S. Lin and W.W. Peterson, Some results on weight distributions of BCH codes, PGIT 12 (1966) 274.
[56] T. Kasami and N. Tokura, On the weight structure of Reed–Muller codes, PGIT 16 (1970) 752–759.
[57] T. Kasami, N. Tokura and S. Azumi, On the weight distribution of Reed–Muller codes, Inst. Electron. Comm. Eng., Japan, PGIT Rept. (1971) (in Japanese).

[58] W.H. Kautz and K.N. Levitt, A survey of progress in coding theory in the Soviet Union, PGIT 15 (1969) 197–244.
[59] V.N. Koshelev, Some properties of random group codes of large length, Probl. Peredači Inform. 1 (1965) 45–48.
[60] M.V. Kozlov, The correcting capacities of linear codes, Soviet Physics – Doklady 14 (1969) 413–415.
[61] J. Leech. Some sphere packings in higher space, Can. J. Math. 16 (1964) 657–682.
[62] J. Leech, Notes on sphere packings, Can. J. Math. 19 (1967) 251–267.
[63] J. Leech and N.J.A. Sloane, New sphere packings in dimensions 9–15, Bull. Amer. Math. Soc. 76 (1970) 1006–1010.
[64] J. Leech and N.J.A. Sloane, New sphere packings in more than thirty-two dimensions, in: Proc. second Chapel Hill Conference on Comb. Math., Chapel Hill, N.C. (1970) 345–355.
[65] J. Leech and N.J.A. Sloane, Sphere packing and error-correcting codes, Can. J. Math 23 (1971) 718–745.
[66] V.K. Leont'ev, A hypothesis on Bose–Chaudhuri codes, Probl. Peredači Inform. 4 (1968) 66–70.
[67] S. Lin and E.J. Weldon Jr., Long BCH codes are bad, IC 11 (1967) 445–451.
[68] C.L. Liu, B.G. Ong and G.R. Ruth. A construction scheme for linear and nonlinear codes, in: Proc. 5th Ann. Princeton Conf. Inform. Sci. (1971) 245–247.
[69] R.W. Lucky, J. Salz and E.J. Weldon Jr., Principles of data communication (McGraw Hill, New York, 1968).
[70] F.J. MacWilliams, Error-correcting codes – An historical survey, in: H.B. Mann, ed., Error correcting codes (Wiley, New York, 1968).
[71] F.J. MacWilliams, Codes and ideals in group algebras, in: R.C. Bose and T.A. Dowling, eds., Combinatorial mathematics and its applications (Univ. North Carolina Press, Chapel Hill, 1969) Ch. 18.
[72] F.J. MacWilliams, Binary codes which are ideals in the group algebra of an abelian group, BSTJ 49 (1970) 987–1011.
[73] F.J. MacWilliams, C.L. Mallows and N.J.A. Sloane, Generalizations of Gleason's theorem on weight enumerators of self-dual codes, PGIT 18 (1972), to appear.
[74] F.J. MacWilliams, N.J.A. Sloane and J.G. Thompson, On the existence of a projective plane of order 10, JCT, to appear.
[75] F.J. MacWilliams, N.J.A. Sloane and J.G. Thompson, Good self-dual codes exist, Discrete Math. 3 (1972) 153–162 (this issue).
[76] A.S. Marchukov, Summation of the product of codes, Probl. Peredači Inform. 4 (1968) 8–15.
[77] R.J. McEliece, On the symmetry of good nonlinear codes, PGIT 16 (1970) 609–611.
[78] R.J. McEliece and H. Rumsey, Jr., Euler products, cyclotomy, and coding, in: Space programs summary (Jet Propulsion Lab., Calif. Inst. Technol.) Vol. 37-65-III (1970) 22–27; and J. Number Theory 4 (1972) 302–311.
[79] D.E. Muller, Application of boolean algebra to switching circuit design and error detection, IRE Trans. Electronic Computers, EC3 (1954) 6–12.
[80] M. Nadler, A 32-point $n = 12$, $d = 5$ code, PGIT 8 (1962) 58.
[81] S.Sh. Oganesyan and V.G. Yagdzhyan, Weight spectra for some classes of cyclic error-correcting codes, Probl. Peredači Inform. 6 (1970) 31–37 (in Russian).
[82] E.T. Parker and P.J. Nikolai, A search for analogues of the Mathieu groups, Math. Comp. 12 (1958) 38–43.
[83] A.M. Patel, Maximal codes with specified minimum distance, IBM Tech. Rept. TR 44.0085 (1969).
[84] A.M. Patel, Maximal group codes with specified minimum distance, IBM J. Res. Devel. 14 (1970) 434–443.

[85] W.K. Pehlert Jr., Analysis of a burst-trapping error correction procedure, BSTJ 49 (1970) 493–519.
[86] W.W. Peterson, On the weight structure and symmetry of BCH codes, Air Force Cambridge Res. Lab., Bedford, Mass., Rept. AFCRL-65-515, 1965.
[87] V.S. Pless, On the uniqueness of the Golay codes, JCT 5 (1968) 215–228.
[88] V.S. Pless, On a new family of symmetry codes and related new five-designs, Bull. Am. Math. Soc. 75 (1969) 1339–1342.
[89] V.S. Pless, Symmetry codes over GF(3) and new five-designs, JCT 12 (1972) 119–142.
[90] V.S. Pless, A classification of self-orthogonal codes over GF(2), Discrete Math. 3 (1972) 209–246 (this issue).
[91] F.P. Preparata, A new look at the Golay (23, 12) code, PGIT 16 (1970) 510–511.
[92] Proc. Second Intern. Symp. Inform. theory, Tsahkadsor, Armenia, September 1971.
[93] I.S. Reed, A class of multiple-error-correcting codes and the decoding scheme, PGIT 4 (1954) 38–49.
[94] D.V. Sarwate and E.R. Berlekamp, On the weight enumeration of Reed–Muller codes and their cosets, to appear.
[95] J.E. Savage, The complexity of decoders, II, Computational work and decoding time, PGIT 17 (1971) 77–85.
[96] N.V. Semakov and V.A. Zinov'ev, Balanced codes and tactical configurations, Probl. Peredači Inform. 5 (1969) 28–36. (in Russian).
[97] N.V. Semakov, V.A. Zinov'ev and G.V. Zaicev, Uniformly packed codes, Probl. Peredači Inform. 7 (1971) 38–50 (in Russian).
[98] C.E. Shannon, A mathematical theory of communication, BSTJ 27 (1948) 379–423, 623–656.
[99] S.G.S. Shiva, Certain group codes, Proc. IEEE 55 (1967) 2162–2163.
[100] V.M. Sidel'nikov, Weight spectra of binary Bose–Chaudhuri–Hocquenghem codes, Probl. Peredači Inform. 7 (1971) 14–22 (in Russian).
[101] R. Singleton, Maximum distance Q-nary codes, PGIT 10 (1964) 116–118.
[102] N.J.A. Sloane, A survey of recent results in constructive coding theory, in: National Telemetering Conf. NTC'71 Record (IEEE, New York, 1971) 218–227.
[103] N.J.A. Sloane and R.J. Dick, On the enumeration of cosets of first order Reed–Muller codes, IEEE Intern. Conf. Communications (Montreal, 1971) 7 (1971) 36–2 to 36–6.
[104] R. Stanton, The Mathieu groups, Can. J. Math. 3 (1951) 164–174.
[105] J.J. Stiffler, Theory of synchronous communications (Prentice-Hall, Englewood Cliffs, N.J., 1971).
[106] M. Sugino, Y. Ienaga, N. Tokura and T. Kasami, Weight distribution of (128, 64) Reed–Muller code, PGIT 17 (1971) 627–628.
[107] A. Tietäväinen, On the nonexistence of perfect codes over finite fields, SIAM J, to appear.
[108] A. Tietäväinen and A. Perko, There are no unknown perfect binary codes, Ann. Univ. Turku, Ser. AI 148 (1971) 3–10.
[109] S.Y. Tong, Burst-trapping techniques for a compound channel, PGIT 15 (1969) 710–715.
[110] S.Y. Tong, Performance of burst-trapping codes, BSTJ 49 (1970) 477–491.
[111] J.H. van Lint, Coding theory, Lecture Notes in Math. 201 (Springer, Berlin, 1971).
[112] J.H. van Lint, A survey of recent work on perfect codes, Rocky Mountain J. Math., to appear.
[113] J.H. van Lint, A new description of the Nadler code, PGIT to appear.
[114] H.C.A. van Tilborg, Weights in the third-order Reed–Muller codes, Jet Propulsion Lab., Calif. Inst. Technol., Tech. Rept. 32–1526, IV, 1971.
[115] E.J. Weldon, Jr., Long quasi-cyclic codes are good (abstract) PGIT 16 (1970) 130.
[116] E. Witt, Über Steinersche Systeme, Abh. Math. Sem. Univ. Hamburg 12 (1938) 265–275.
[117] J.K. Wolf, Adding two information symbols to certain nonbinary BCH codes and some applications, BSTJ 48 (1969) 2405–2424.
[118] J.K. Wolf, Nonbinary random error-correcting codes, PGIT 16 (1970) 236–237.