New Family of Single-Error Correcting Codes

NEIL J. A. SLOANE, MEMBER, IEEE, AND DONALD S. WHITEHEAD, MEMBER, IEEE

Abstract—A construction is given that combines an (n, M_1, d_1) code with an $(n, M_2, d_2 = [\frac{1}{2}(d_1 + 1)])$ code to form a $(2n, M_1M_2, d_1)$ code. This is used to construct a new family of nongroup single-error correcting codes of all lengths n from 2^m to $3 \cdot 2^{m-1} - 1$, for every $m \geq 3$. These codes have more codewords than any group code of the same length and minimum distance. A number of other nongroup codes are also obtained. Examples of the new codes are (16,2560,3) and (16,36,7) codes, both having more codewords than any comparable group code.

I. Introduction

ONLY A FEW binary nongroup codes are known that have more codewords than any group code. Examples are the single-error correcting codes of Golay [2] and Julin [5] of lengths 8–11; the double-error correcting codes of Nadler [7], Green [3], Nordstrom and Robinson [8], and Preparata [11], of lengths 12–15 and $4^m - 1$, $m \geq 3$; and codes based on Hadamard matrices ([1], p. 317).

In Section III we give a simple description of the codes of Golay and Julin and extend them to obtain nongroup single-error correcting codes of all lengths from 2^m to $3 \cdot 2^m - 1$, $m \geq 3$, which have more codewords than any group code of the same length and minimum distance.

The extension is carried out by means of a construction (given in Section II) that combines an (n, M_1, d_1) code with an $(n, M_2, d_2 = [\frac{1}{2}(d_1 + 1)])$ code to give a $(2n, M_1M_2, d_1)$ code. In Section IV we construct a family of nongroup quadratic residue codes of high minimum distance. Finally, in Section V the main construction is used to generate recursively all Reed–Muller codes of lengths 2^m, and to generate triple-error correcting codes of lengths 32–47.

Throughout, an (n, M, d) code denotes a set of M binary vectors of length n of Hamming distance at least d apart.

II. Construction

The heart of the construction is an operator $\oplus$ that sends pairs of binary vectors of length n to binary vectors of length $2n$, defined by

$$(x_1, x_2, \cdots, x_n) \oplus (y_1, y_2, \cdots, y_n) = (x_1 + y_1, \cdots, x_n + y_n, y_1, \cdots, y_n),$$

where $+$ is the ordinary addition modulo 2.

This is extended to the construction for codes. Let $\mathcal{C}_1 = (n, M_1, d_1)$ and $\mathcal{C}_2 = (n, M_2, d_2 = [\frac{1}{2}(d_1 + 1)])$ be two codes. Then the new code, denoted by $\mathcal{C}_1 \oplus \mathcal{C}_2$, is

$$\mathcal{C}_1 \oplus \mathcal{C}_2 = \{x \oplus y, \quad x \in \mathcal{C}_1, \quad y \in \mathcal{C}_2\}.$$

An informal description is that the codewords of $\mathcal{C}_1 \oplus \mathcal{C}_2$ are obtained by adding an arbitrary codeword of $\mathcal{C}_1$ to an arbitrary codeword of $\mathcal{C}_2$, and appending a copy of the codeword of $\mathcal{C}_2$.

Theorem 1: $\mathcal{C}_1 \oplus \mathcal{C}_2$ is a $(2n, M_1M_2, d_1)$ code.

Proof: Every choice of codeword $\boldsymbol{x} \in \mathcal{C}_1$ and $\boldsymbol{y} \in \mathcal{C}_2$ gives rise to a different codeword $\boldsymbol{x} \oplus \boldsymbol{y}$, so the new code has M_1M_2 codewords. To show that the distance between $\boldsymbol{x}_1 \oplus \boldsymbol{y}_1$ and $\boldsymbol{x}_2 \oplus \boldsymbol{y}_2$ is at least d_1, in the case $\boldsymbol{x}_1 \neq \boldsymbol{x}_2$ then $\boldsymbol{x}_1$ and $\boldsymbol{x}_2$ differ in at least d_1 places and so do $\boldsymbol{x}_1 \oplus \boldsymbol{y}_1$ and $\boldsymbol{x}_2 \oplus \boldsymbol{y}_2$. On the other hand, if $\boldsymbol{x}_1 = \boldsymbol{x}_2$ and $\boldsymbol{y}_1 \neq \boldsymbol{y}_2$ then by the construction the distance between $\boldsymbol{x}_1 \oplus \boldsymbol{y}_1$ and $\boldsymbol{x}_1 \oplus \boldsymbol{y}_2$ is exactly twice the distance between $\boldsymbol{y}_1$ and $\boldsymbol{y}_2$ and so is $\geq 2d_2 \geq d_1$.

Remarks

1) Since $(x \oplus y) + (x' \oplus y') = (x + x') \oplus (y + y')$ (the $+$ denoting component-wise addition modulo 2), if $\mathcal{C}_1$ and $\mathcal{C}_2$ are group codes then so is $\mathcal{C}_1 \oplus \mathcal{C}_2$. But $\mathcal{C}_1 \oplus \mathcal{C}_2$ need not be cyclic even when $\mathcal{C}_1$ and $\mathcal{C}_2$ are.

2) The construction can be applied to codes over any field, and Theorem 1 will still hold.

3) Since discovering this construction it has been pointed out to us by Elspas that an equivalent construction was given by Plotkin [10] for the case when d_1 is even. Since then it has been almost unnoticed, and it seems to be worthwhile restating the construction in its general form. It is not mentioned, for example, by Berlekamp in his survey of methods of combining codes ([1], ch. 14).

A similar construction with lower minimum distance is given by Slepian ([12], [1], p. 347), in which (n_1, M_1, d_1) and (n_2, M_2, d_2) codes are concatenated to form the direct sum $(n_1 + n_2, M_1M_2, d = \min(d_1, d_2))$ code.

III. New Family of Single-Error Correcting Codes

The sphere-packing bound for an $(n, M, 3)$ single-error correcting code is

$$M \leq 2^n/(1 + n). \tag{1}$$

For n of the form $n = 2^m - 1$, this bound is attained by the Hamming $(2^m - 1, 2^{2^m-m-1}, 3)$ codes. If $l - 1$ information symbols of a Hamming code are set to zero, the shortened Hamming codes

$$(2^m - l, 2^{2^m-m-l}, 3)$$

are obtained. These are known [4] to have the maximum

Manuscript received February 23, 1970.

N. J. A. Sloane is with Bell Telephone Laboratories, Inc., Murray Hill, N. J. 07974.

D. S. Whitehead is with the School of Electrical Engineering, Cornell University, Ithaca, N. Y. 14850.

number of codewords of any group or nongroup code when $n = 4, 5$, and $2^m - 2$, $m \geq 3$; and from (1) it follows that they have the maximum number of codewords of any single-error correcting *group* code of any length n.

Golay and Julin Codes

For lengths 8–11, single-error correcting nongroup codes containing more codewords than shortened Hamming codes were given by Golay [2] and Julin [5]. Their codes may be obtained as follows.

Let $\mathfrak{D}$ be the (11×11) binary circulant matrix whose first row is 11011100010, containing 1's at 0 and at the quadratic residues of 11. Let $\mathfrak{A}$ be the (12×12) binary matrix formed by adding a row and column of 0's to $\mathfrak{D}$.

$$\mathfrak{A} = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & \mathfrak{D} & \\ 0 & & & \end{bmatrix}.$$

Then (for example, see Leech [6]) the sums modulo 2 of pairs of rows of $\mathfrak{A}$, and the complements of such sums, form the 132 vectors of the Steiner system $S(5, 6, 12)$, and thus form a (12, 132, 4) code in which all words have weight 6. Deleting the first coordinate gives a cyclic (11, 132, 3) code with 66 words each of weights 5 and 6. This may be increased to 144 words by adding 1^20^9, $0^21^20^7$, $0^41^20^5$, $0^61^20^3$, 0^81^20, $0^{10}1$ and their complements, giving $\mathcal{C}_{11} = (11, 144, 3)$.

Taking the even-weight codewords of $\mathcal{C}_{11}$ gives an (11, 72, 4) code that contains a cyclic set of 66 words of weight 6. Again deleting a coordinate gives $\mathcal{C}_{10} = (10, 72, 3)$, containing 5 words of weight 2, 36 of weight 5, 30 of weight 6, and 1 of weight 10.

If now one coordinate is deleted from the 36 words of weight 5, and the codewords 0^9, 1^9 added, the code $\mathcal{C}_9 = (9, 38, 3)$ is obtained. This has the surprising property that by a suitable permutation of the 9 coordinates it can be made into the tricyclic code—i.e., shifting a codeword cyclically by 3 places again gives a codeword—consisting of 0^9, 1^9 and all tricyclic shifts of the row vectors

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

The 18 words of weight 4 in $\mathcal{C}_9$ have Hamming distance 4 among themselves. By deleting a coordinate and adding 0^8 and 1^8 we obtain $\mathcal{C}_8 = (8, 20, 3)$; and by a permutation of the 8 coordinates this can be made into the cyclic code consisting of 0^8, 1^8, $(01)^4$, $(10)^4$, and all cyclic shifts of 11010000 and 11100100.

The *new codes* are now obtained by applying the construction of Section II to $\mathcal{C}_8 - \mathcal{C}_{11}$. Combining $\mathcal{C}_8 = (8, 20, 3)$ with the $(8, 2^7, 2)$ single parity-check code gives a $(16, (5/4)\cdot 2048, 3)$ code, compared to 2048 words for the shortened Hamming code. Combining the extended (9, 20, 4) and the $(9, 2^8, 2)$ code gives an $(18, (5/4)\cdot 2^{12}, 4)$ and thus a $(17, (5/4)\cdot 2^{12}, 3)$. From (9, 38, 3) and $(9, 2^8, 2)$ we obtain an $(18, (19/16)\cdot 2^{13}, 3)$, and so on. Repeated applications of the construction give the following.

Theorem 2: For any block length n satisfying $2^m \leq n < 3\cdot 2^{m-1}$ there exists a nongroup $(n, \lambda 2^{n-m-1}, 3)$ code, where $\lambda = 5/4$, 19/16, or 9/8 accordingly as the binary expansion of n begins $1000 \cdots$, $1001 \cdots$, or $101 \cdots$. λ is the fractional improvement in the number of codewords over the shortened Hamming code.

Remark

Of this family of codes, only the one of length 8 is known to be optimal. For the others, the number of codewords lies below the best-known upper bound [4].

Encoding and decoding of any of the codes of Theorem 2 can be reduced to the finite (but as far as we know, unsolved) problem of encoding and decoding the codes $\mathcal{C}_8 - \mathcal{C}_{11}$. The encoding is done iteratively, following the construction. To illustrate the decoding method, suppose codes $\mathcal{C}_1 = (n, M, 3)$ and $\mathcal{C}_2 = (n, 2^{n-1}, 2)$ were combined by the construction to give $\mathcal{C}_3 = (2n, 2^{n-1}M, 3)$. We will show how to decode $\mathcal{C}_3$ given a decoder for $\mathcal{C}_1$.

Let the received vector be

$$\boldsymbol{y} = (y_{11}, y_{21}, \cdots, y_{n1}, y_{12}, y_{22}, \cdots, y_{n2})$$

and define $P_1(y)$, the projection onto $\mathcal{C}_1$, to be

$$P_1(y) = (y_{11} + y_{12}, y_{21} + y_{22}, \cdots, y_{n1} + y_{n2})$$

and let

$$P_2(y) = \sum_{i=1}^{n} y_{i2}.$$

If no errors occurred, $P_1(y) \in \mathcal{C}_1$ and $P_2(y) = 0$. If some y_{i1} is in error, $P_1(y)$ will have a single error in position i that the decoder for $\mathcal{C}_1$ will find; and $P_2(y) = 0$. On the other hand, if some y_{i2} is in error, again the decoder for $\mathcal{C}_1$ finds i, and now $P_2(y) = 1$. Thus, any single error can be corrected.

IV. Family of Nongroup Quadratic Residue Codes

Let n be a prime of the form $n = 4m + 1$. Define vectors $\boldsymbol{a}$ and $\boldsymbol{b}$ by $\boldsymbol{a} = (a_0, a_1, \cdots, a_{n-1})$ where $a_0 = 0$, $a_i = 1$ if i is a quadratic residue modulo n, $a_i = 0$ otherwise; and $\boldsymbol{b} = (b_0, b_1, \cdots, b_{n-1})$ where $b_0 = 0$ and $b_i = 1 - a_i$ for $1 \leq i \leq n - 1$. Let $\mathcal{C}$ be the code consisting of 0^n, 1^n, and all $2n$ cyclic shifts of $\boldsymbol{a}$ and $\boldsymbol{b}$.

Theorem 3: $\mathcal{C}$ is an $(n = 4m + 1, M = 8m + 4, d = 2m)$ cyclic nongroup code.

Proof: An easy consequence of Theorems 3 and 4 of Perron [9].

Remark

For $m = 1$ and 3, $\mathcal{C}$ is an inferior code. For $m = 4$, we obtain (17, 36, 8) and (16, 36, 7) codes, which by the Johnson 1954 bound have more codewords than any comparable group code (see [4]). For larger m it is not known how good these codes are, although they have more codewords than any comparable group code presently known.

V. Other Applications

Reed–Muller Codes

The construction of Section II generates all the Reed–Muller (RM) codes recursively. Let $\mathcal{C}_1$ be an rth-order RM code of length 2^m, with $k = 1 + \binom{m}{1} + \cdots + \binom{m}{r}$ information symbols and minimum distance $d = 2^{m-r}$; and let $\mathcal{C}_2$ be an $(r + 1)$th-order RM code of the same length. Then $\mathcal{C}_1 \oplus \mathcal{C}_2$ is a code of length 2^{m+1}, with

$$k = 1 + \binom{m}{1} + \cdots + \binom{m}{r} + 1 + \binom{m}{1} + \cdots + \binom{m}{r+1} = 1 + \binom{m+1}{1} + \cdots \binom{m+1}{r+1},$$

and $d = 2^{m-r}$, which can be shown to be the $(r + 1)$th-order RM code of this length. (We omit the details of the proof.)

Triple-Error Correcting Codes

As a final example, we apply the construction with $\mathcal{C}_1$ successively taken to be the (16, 36, 7) code of Section IV and the $(n, 2^{n-11}, 7)$ shortened Golay codes for $17 \leq n \leq 23$, and with $\mathcal{C}_2$ equal to the corresponding $(n, \lambda 2^{n-6}, 4)$ codes of Section III. We obtain a family of $(n, \lambda 2^{n-17}, 7)$ codes that for $n = 32$ ($\lambda = 9/4$), $n = 40$ ($\lambda = 19/16$), and $41 \leq n \leq 47$ ($\lambda = 9/8$) appear to contain more codewords than any comparable group code presently known. For lengths 33–39, however, these codes are inferior to the $(n, 2^{n-16}, 7)$ group codes recently discovered by Leech (see [13]).

Acknowledgment

The authors wish to thank E. R. Berlekamp, B. Elspas, and J. Leech for their helpful suggestions.

Bibliography

[1] E. R. Berlekamp, *Algebraic Coding Theory*. New York: McGraw-Hill, 1968.
[2] M. J. E. Golay, "Binary coding," *IEEE Trans. Information Theory*, vol. PGIT-4, pp. 23–28, September 1954.
[3] M. V. Green, "Two heuristic techniques for block-code construction," *IEEE Trans. Information Theory* (Abstract), vol. IT-12, p. 273, April 1966.
[4] S. M. Johnson, "On upper bounds for unrestricted error correcting codes," RAND Rept. RM-5716-PR, December 1968.
[5] D. Julin, "Two improved block codes," *IEEE Trans. Information Theory* (Correspondence), vol. IT-11, p. 459, July 1965.
[6] J. Leech, "Some sphere packings in higher space," *Can. J. Math.*, vol. 16, pp. 657–682, 1964.
[7] M. Nadler, "A 32-point $n = 12$, $d = 5$ code," *IRE Trans. Information Theory* (Correspondence), vol. IT-8, p. 58, January 1962.
[8] A. W. Nordstrom and J. P. Robinson, "An optimum nonlinear code," *Inform. and Control*, vol. 11, pp. 613–616, 1967.
[9] O. Perron, "Bemerkungen über die Verteilung der quadratischen Reste," *Math. Z.*, vol. 56, 122–130, 1952.
[10] M. Plotkin, "Binary codes with specified minimum distance," *IEEE Trans. Information Theory*, vol. IT-6, pp. 445–450, September 1960.
[11] F. P. Preparata, "A class of optimum nonlinear double-error-correcting codes," *Inform. and Control*, vol. 13, pp. 378–400, 1968.
[12] D. Slepian, "Some further theory of group codes," *Bell Sys. Tech. J.*, vol. 39, pp. 1219–1252, 1960.
[13] J. Leech and N. J. A. Sloane, "Sphere packings and error-correcting codes" (to be published).