

# BINARY CODES WITH DISJOINT CODEBOOKS AND MUTUAL HAMMING DISTANCE

Indexing term: Error-correction codes

Equal-length linear binary block error-control codes with disjoint codebooks and mutual Hamming distance are considered. A method of constructing pairs of these disjoint codes from known cyclic codes, and determining their mutual distance, is described. Some sets of length-15 cyclic codes are tabulated.

The author is concerned with the construction of sets of equal-length linear binary block error-control codes with disjoint codebooks for use in several coding schemes.<sup>1</sup> In addition, for any pair of disjoint codes, it is required to find the minimum distance that separates the words of one code from the words of the other. This distance is called the minimum mutual Hamming distance  $d_m$  of the disjoint code pair. This letter establishes the conditions which a pair of codes must fulfil if they are to have disjoint codebooks, and gives a general method for calculating  $d_m$ . In particular, a practical method of testing pairs of known cyclic codes for disjoint codebooks, and determining their mutual distance, is described.

An  $(n, k, d)$  binary linear block code has length  $n$ , a codebook of  $2^k$  codewords (including the all-zero word) and minimum distance  $d$  equal to the weight of the minimum-weight nonzero codeword. The code is completely specified by a  $k \times n$  generator matrix  $G$  whose rows are linearly independent basis vectors that span the codespace. Each of the  $2^k$  distinct linear combinations of rows of  $G$  generates a distinct codeword.

Consider two codes  $C_1$  and  $C_2$  with parameters  $(n, k_1, d_1)$  and  $(n, k_2, d_2)$  and generator matrices  $G_1$  and  $G_2$ . For  $C_1$  and  $C_2$  to have disjoint codebooks, apart from the all-zero word, no codeword in  $C_1$  must equal a codeword in  $C_2$ . That is, no linear combination of rows of  $G_1$  equals a linear combination of rows of  $G_2$ , and therefore the rows of  $G_1$  and  $G_2$  must be mutually linearly independent. A matrix  $G_c$  that has as rows all the basis vectors of  $C_1$ , all the basis vectors of  $C_2$  and no others, must therefore have  $k_1+k_2$  linearly independent rows if  $C_1$  and  $C_2$  are to be disjoint, and can therefore be considered as the generator matrix of an  $(n, k_1+k_2, d_c)$  code, which will be called the common code  $C_c$ . A necessary condition for the rows of  $G_c$  to be linearly independent, and hence for  $C_1$  and  $C_2$  to be disjoint, is

$$n \geq k_1 + k_2 \quad (1)$$

Table 1

$k_1$	$k_2$	$d_1$	$d_2$	Roots $g_1(x)/g_2(x)$	Roots $g_c(x)$	$k_c$	$d_m$
9	6	4	6	3, 5/0, 1, 7	-	15	1
9	4	4	6	3, 5/0, 1, 5, 7	5	13	2
9	2	3	10	1, 5/0, 1, 3, 7	1	11	3
8	6	4	6	0, 3, 5/0, 1, 7	0	14	2
8	2	4	10	0, 3, 5/0, 1, 3, 7	0, 3	10	2
8	2	4	10	0, 1, 5/0, 1, 3, 7	0, 1	10	4
7	4	3	8	1, 7/0, 1, 3, 5	1	11	3
7	4	5	6	1, 3/0, 1, 5, 7	1	11	3
6	5	6	7	0, 1, 3/1, 5, 7	1	11	3
6	4	6	8	0, 1, 7/0, 1, 3, 5	0, 1	10	4
5	4	3	8	1, 5, 7/0, 1, 3, 5	1, 5	9	3
5	2	7	10	1, 3, 5/0, 1, 3, 7	1, 3	7	5
4	4	6	8	0, 1, 5, 7/0, 1, 3, 5	0, 1, 5	8	4
4	3	8	10	0, 1, 3, 5/1, 3, 7	1, 3	7	5
4	2	8	10	0, 1, 3, 5/0, 1, 3, 7	0, 1, 3	6	6

Given that eqn. 1 is satisfied and that the rows of  $G_c$  are linearly independent, it can be shown that the minimum distance  $d_c$  of the common code equals the minimum mutual distance  $d_m$  of the code pair. The sum of any  $C_1$  word  $u_1$  with any  $C_2$  word  $u_2$  equals a third word  $u_{12}$ , and the weight of this 'mutual' word equals the mutual distance between  $u_1$  and  $u_2$ . The minimum mutual distance between the codes then

equals either the minimum-weight nonzero  $C_1$  word, the minimum-weight nonzero  $C_2$  word, or the minimum-weight mutual word, whichever is smaller. The common code contains all these words, plus the all-zero word, and no other. The minimum distance of the common code therefore equals the minimum mutual distance, which can never exceed  $d_1$  or  $d_2$ , whichever is smaller. A necessary and sufficient condition for disjoint codebooks is therefore that the common code should have a distance  $\geq 1$ .

To test two codes for disjoint codebooks, the individual codes are tested for mutually linearly independent basis vectors, and  $d_m$  is determined by finding the distance of the common code. These procedures are, however, impractically lengthy, even with computer aid, if  $k_1$  and  $k_2$  are large. The converse procedure, that of partitioning a known common code-generator matrix to yield two useful disjoint codes is attractive, and is at present under investigation. The problems involved in testing for disjoint codes and determining  $d_m$  are simplified if  $C_1$  and  $C_2$  are nontrivial ( $k_1, k_2 \neq 0, \neq n$ ) cyclic codes. In this case, we consider the generator polynomials  $g_1(x)$  and  $g_2(x)$  of  $C_1$  and  $C_2$ , with degrees  $n-k_1$  and  $n-k_2$ , respectively. A generator polynomial can be characterised by a list of the exponents of its roots, or written as a polynomial whose irreducible factors are minimum functions of its constituent roots.<sup>2</sup> The  $2^k$  codewords in a cyclic code consist of all multiples  $u(x) = m(x)g(x)$ , where  $m(x)$  is a message polynomial of degree  $\leq k-1$ . For  $C_1$  and  $C_2$  to have disjoint codebooks, a word  $u_1$  in  $C_1$  must not be exactly divisible by  $g_2(x)$ . That is,

$$\frac{m_1(x)g_1(x)}{g_2(x)} \dots \dots \dots (2)$$

must have a nonzero remainder. Eqn. 2 therefore requires that the degree of  $m_1(x)$  is less than the degree of  $g_2(x)$  giving

$$n - k_2 > k_1 - 1 \quad \text{and} \quad n > k_1 + k_2 - 1 \quad (3)$$

as a necessary condition for disjoint codebooks.

Because the factors of  $g_1(x)$  and  $g_2(x)$  are factors of  $x^n+1$ ,  $g_1(x)$  and  $g_2(x)$  may have common factors that will cancel in eqn. 2. A further necessary condition is then that, after cancellation of common factors, the denominator of eqn. 2 must still have a higher degree than  $m_1(x)$ . The largest denominator after cancellation occurs when  $g_2(x)$  contains all the factors of  $x^n+1$  that do not appear in  $g_1(x)$ . The degree of the resultant denominator is then at least  $k_1$ , which is the minimum degree required for the denominator to have degree greater than  $k_1-1$ , the degree of  $m_1(x)$ . The

conditions required for two cyclic codes to have disjoint codebooks are therefore (a)  $k_1, k_2 \neq 0, \neq n$ , (b)  $n > k_1 + k_2 - 1$ , and (c)  $g_1(x)$  and  $g_2(x)$  between them contain all the irreducible factors of  $x^n+1$ .

The generator of the common code,  $g_c(x)$ , must divide  $g_1(x)$ ,  $g_2(x)$  and all mutual words only, and is therefore the greatest common divisor of  $g_1(x)$  and  $g_2(x)$ . The common

code is also cyclic, so that its distance, and hence the mutual distance of the disjoint code pair, is easily determined if the code is tabulated.<sup>2</sup> If the distance of the common code is not known exactly, a lower bound on mutual distance can be obtained by the Bose-Chaudhuri-Hocquenghem (BCH) bound for cyclic codes.<sup>2</sup> The converse procedure, that of constructing a disjoint code pair, is also considerably simplified: a common code is first selected, defining  $d_m$ , and factors are added to  $g_1(x)$  and  $g_2(x)$ , subject to conditions (a) to (c), to produce the required codes. Similarly, a code disjoint to an existing code can be easily constructed. Sets of more than two disjoint codes can also be formed by repeated construction of disjoint pairs. These procedures for the testing and construction of disjoint cyclic code pairs are practical, and also suitable for computer implementation.

*Example:* It is required to test the (15, 6, 6) code and the (15, 4, 8) code for disjoint codebooks. The exponents of the roots of the generator polynomial are tabulated<sup>2</sup> as (0, 1, 7) and (0, 1, 3, 5), respectively. Condition (a) is satisfied; condition (b) is satisfied:  $15 > 6 + 4 - 1$ ; and condition (c) is satisfied because all the roots of  $x^{15} + 1$  are contained in  $g_1(x)$  and  $g_2(x)$ . The codebooks are therefore disjoint. The roots (0, 1) are common and cancel, leaving (3, 5) as the roots of the denominator. The minimum functions of 3 and 5 have degrees 4 and 2, respectively, giving a denominator of degree 6, which is greater than 5, the degree of  $m_1(x)$ . The roots of  $g_c(x)$  are (0, 1), and the common code is therefore the (15, 10, 4) code, giving  $d_m = 4$ . Table 1 gives some of the length-15 disjoint code pairs with mutual Hamming distances.

R. M. F. GOODMAN

5th August 1974

School of Electronic Engineering  
Kingston Polytechnic  
Penrhyn Road, Kingston upon Thames, Surrey, England

#### References

- GOODMAN, R. M. F.: 'Variable redundancy coding'. Ph.D thesis' University of Kent at Canterbury (in preparation)
- PETERSON, W. W., and WELDON, E. J., JUN.: 'Error-correcting codes' (MIT Press, 1972)

## GOOD BLOCK CODES DERIVED FROM CYCLIC CODES

*Indexing term: Error-correction codes*

By combining irreducible cyclic codes, we obtain good quasicyclic or extended quasicyclic codes. Some of these improve on the lower bound of Helgert and Stinaff.

Let  $\varepsilon(X)$  be the idempotent generator of an irreducible  $(n', k', d')$  cyclic block code, whose parity-check polynomial is  $h(X)$ , and let  $f(X)$  be a primitive polynomial for the field of polynomials modulo  $h(X)$ . We now construct an  $(n = vn', k = k')$  quasicyclic block code, with one generator  $g(X, D)$  that can be written as

$$g(X, D) = \sum_{j=0}^{v-1} D^j \varepsilon(X) [f(X)]^{b(j)} \text{ modulo } (X^n - 1) \quad (1)$$

Since any information  $k$ -tuple  $i(X)$  can be represented by  $[f(X)]^{\beta[i(X)]}$  modulo  $h(X)$ , for a well chosen integer  $\beta[i(X)]$ , the encoding of  $i(X)$  results in

$$i(X)g(X, D) = \sum_{j=0}^{v-1} D^j \varepsilon(X) [f(X)]^{b(j) + \beta[i(X)]} \quad (2)$$

that is, taken modulo  $X^n - 1$ . The minimal weight  $d$  of a nonzero word, such as in eqn. 2, is at least  $vd'$ , but it can be larger for a good choice of  $b(j)$ . A method was recently sketched<sup>5</sup> that can be used to choose the best function  $b(j)$  and to analyse the weight distribution of the obtained codes. It uses some results of Goethals,<sup>2</sup> and is not recalled here.

We can also generalise the present construction by using several generators such as in eqn. 1 or by adding a parity-check digit to the elementary  $n'$ -tuples. In the following,  $\mathcal{J}(X)$  denotes the all one  $n'$ -tuple and  $\mathcal{J}_p(X)$  is obtained by adding a parity-check digit to  $\mathcal{J}(X)$ . Many cyclic codes were tested for this construction (sometimes with a computer), and we now summarise the cases where the lower bound of Helgert and Stinaff<sup>3</sup> was improved. We use  $A_i$  to denote the number of vectors of weight  $i$ . The codes indexed by \* were implicitly constructed in Reference 5 and  $d_{HS}$  is the bound on the minimum distance<sup>3</sup> of the best linear  $(n, k)$  code.

$$(a) \quad n' = 17 \quad \varepsilon(X) = \sum_{i=0}^7 (X^3)^{2^i}$$

$$g_1(X, D) = \varepsilon(X) + D(1 + X)^5 \varepsilon(X)$$

$$(n, k, d) = (34, 8, 14) \quad 13 \leq d_{HS} \leq 14^*$$

(b) cfr (a) with a second generator

$$g_2(X, D) = \mathcal{J}_p(X)$$

$$(n, k, d) = (35, 9, 14) \quad 13 \leq d_{HS} \leq 14$$

$$(c) \quad n' = 21 \quad \varepsilon(X) = X^7 + X^{14} + \sum_{i=0}^5 X^{2^i}$$

$$g_1(X, D) = \varepsilon(X) + D(1 + X)\varepsilon(X)$$

$$g_2(X, D) = \mathcal{J}_p(X) \quad g_3(X, D) = D\mathcal{J}_p(X)$$

$$(n, k, d) = (44, 8, 18) \quad 17 \leq d_{HS} \leq 20$$

$$(d) \quad n' = 39 \quad \varepsilon(X) = \sum_{i=0}^{11} (X^3 + X^7)^{2^i}$$

$$g_1(X, D) = \varepsilon(X) + D(X^2 + X + 1)^{15} \varepsilon(X)$$

$$g_2(X, D) = \mathcal{J}_p(X) \quad g_3(X, D) = D\mathcal{J}_p(X)$$

$$(n, k, d) = (80, 14, 32) \quad 29 \leq d_{HS} \leq 34$$

$$\text{Weight distribution: } A_0 = A_{80} = 1$$

$$A_{32} = A_{48} = 2535$$

$$A_{40} = 11312$$

$$(e) \quad n' = 55 \quad \varepsilon(X) = \sum_{i=0}^3 X^{(11)^{2^i}} + \sum_{i=0}^{19} (X^3)^{2^i}$$

$$g_1(X, D) = \varepsilon(X) + D(X^3 + X + 1)^{1271} \varepsilon(X)$$

$$(n, k, d) = (110, 20, 40) \quad 36 \leq d_{HS} \leq 46$$

Weight distribution:

$$A_0 = 1, A_{40}^* = 109, A_{44}^* = 676, A_{48}^* = 2285$$

$$A_{52}^* = 5028, A_{56}^* = 5630, A_{60}^* = 3724$$

$$A_{64}^* = 1291, A_{68}^* = 300, A_{72}^* = 21, A_{76}^* = 0$$

$$A_{80}^* = 1 \quad \text{where } A_i^* \text{ denotes } A_{i/55}$$

By using MacWilliams's equations,<sup>1</sup> we check that the minimum weight of the dual code is 5. The present code can thus be shortened to obtain a (105, 20) code with

$$d = 36 \quad (32 \leq d_{HS} \leq 44).$$

$$(f) \quad n' = 41 \quad \varepsilon(X) = \sum_{i=0}^{19} X^{2^i}$$

$$g_1(X, D) = \varepsilon(X) + D\varepsilon(X)(X^3 + X + 1)^{253}$$

$$(n, k, d) = (82, 20, 26) \quad 24 \leq d_{HS} \leq 32$$

$$(g) \quad n' = 51 \quad \varepsilon(X) = \sum_{i=0}^7 (X + X^3 + X^5 + X^{19})^{2^i}$$

$$g_1(X, D) = \varepsilon(X) + D\varepsilon(X)(1 + X)^3$$

$$g_2(X, D) = \varepsilon(X^{11}) + D\varepsilon(X^{11})(1 + X)^{37}$$

$$g_3(X, D) = \mathcal{J}_p(X) \quad g_4(X, D) = D\mathcal{J}_p(X)$$

$$(n, k, d) = (102, 18, 36) \quad 32 \leq d_{HS} \leq 43$$