View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Elsevier - Publisher Connector

© DISCRETE MATHEMATICS 4 (1973) 171–184. North-Holland Publishing Company

A CONSTRUCTION SCHEME FOR LINEAR AND NON-LINEAR CODES

C.L. LIU, B.G. ONG and G.R. RUTH

Department of Computer Science, University of Illinois, Urbana, Ill., USA

Department of Mathematics, Queens University, Kingston, Ont., Canada

Department of Electrical Engineering, Massachusetts Institute of Technology, Cambridge, Mass., USA

Received 11 February 1971

Abstract. A scheme for construcing linear and non-linear codes is presented. It constructs a code of block length $2n$ from two constituent codes of block length n. Codes so constructed can be either linear or non-linear even when the constituent codes are linear. The construction of many known linear and non-linear codes using this scheme will be shown.

1. Introduction

The discovery of non-linear codes that are superior to known linear codes has generated a great deal of interest in studying the structure of non-linear codes as well as methods for constructing them. However, since non-linear codes are defined for their lack of a certain mathematical structure (the codewords do not form a linear vector space), to obtain a general mathematical description of non-linear codes is a rather difficult task. Consequently, our knowledge on how to construct non-linear codes is quite limited. In this paper, we present a scheme for constructing linear and non-linear codes which we hope will also shed some light on the mathematical structure of non-linear codes.

2. The construction scheme

Our scheme constructs a $(2n, q^n)$ q-ary code[1] from two q-ary codes

[1] We use the term "an (n, M) code" and "an (n, M, d) code" to refer to a block code with block length n, distance d, and M codewords.

which we shall call the constituent codes. Let G_1 be an (n, q^k) q-ary linear code of distance d_1. Let G_2 be an (n, q^{n-k}) q-ary code of distance d_2. Since G_1 is a linear code, we can divide the set of all ordered q-ary n-tuples into distinct cosets of G_1. Clearly, there are q^{n-k} cosets. We assign to each coset a codeword of G_2. We now construct a $(2n, q^n)$ systematic code G as follows: Let i be a q-ary information word of n digits. Let $f(i)$ denote the codeword of G_2 that is assigned to the coset of G_1 containing i. The encoded word for i in G is then the concatenation of the two words i and $i + f(i)$, denoted by $(i, i + f(i))$.

Let us illustrate the construction procedure by a simple example. Let $G_1 = \{000, 110, 011, 101\}$ and $G_2 = \{000, 111\}$ be the two constituent codes. The cosets of G_1 and the codewords of G_2 assigned to them are shown in table 1(a). The encoded words in G are then shown in table 1(b).

Table 1(a)

Cosets of G_1				Assignment of codewords of G_2 to the cosets
000	110	011	101	000
001	111	010	100	111

Table 1(b)

Information words	Encoded words in G
000	000000
001	001110
010	010101
011	011011
100	100011
101	101101
110	110110
111	111000

Theorem 2.1. *The code G constructed above is a $(2n, q^n)$ code whose distance is at least equal to* $\min(2d_1, d_2)$.

Proof. It is clear that the block length of G is $2n$. There are q^n codewords in G, because there are q^n distinct information words.

Let $(i_1, i_1 + f(i_1))$ and $(i_2, i_2 + f(i_2))$ be two codewords in G. To determine the distance between these two words, we examine two cases:

Case 1. i_1 and i_2 are in the same coset of G_1. In this case, $f(i_1) = f(i_2)$. Thus[2]

$$D[(i_1, i_1 + f(i_1)), (i_2, i_2 + f(i_2))] = D[i_1, i_2] + D[i_1, i_2] \geq 2d_1 .$$

Case 2. i_1 and i_2 are not in the same coset of G_1. In this case, $f(i_1) \neq f(i_2)$. Thus,

$$\begin{aligned} D[(i_1, i_1 + f(i_1)), (i_2, i_2 + f(i_2))] &= D[i_1, i_2] + D[i_1 + f(i_1), i_2 + f(i_2)] \\ &\geq D[f(i_1), f(i_2)] = d_2 . \end{aligned}$$

It should be noted that $\min(2d_1, d_2)$ is only a lower bound on the distance of the code G. In particular, if $2d_1 \leq d_2$, then the distance of G is equal to $2d_1$. However, if $2d_1 > d_2$, then $\min(2d_1, d_2)$ is a lower bound on the distance of G. (In the following, we shall see examples in which the distance of G exceeds $\min(2d_1, d_2)$, where $2d_1 > d_2$.)

The code G so constructed can be either linear or non-linear as indicated in the next theorem.

Theorem 2.2. *The code G is linear if and only if the following conditions are satisfied*: (1) $f(ci) = cf(i)$ *for any constant* c;
(2) $f(i_1 + i_2) = f(i_1) + f(i_2)$.

Proof. It is clear that (1) and (2) are sufficient conditions for G to be linear. To show that they are also necessary conditions, we note that:

(1) The encoded word for i is $(i, i + f(i))$. If G is linear, $c(i, i + f(i))$ which is equal to $(ci, ci + cf(i))$ must also be a codeword in G. Since the encoded word of ci is $(ci, ci + f(ci))$, we must have $f(ci) = cf(i)$.

(2) Let $(i_1, i_1 + f(i_1))$ and $(i_2, i_2 + f(i_2))$ be two codewords in G. If G is linear, $(i_1 + i_2, i_1 + i_2 + f(i_1) + f(i_2))$ must also be a codeword. Since the encoded word of $i_1 + i_2$ is $(i_1 + i_2, i_1 + i_2 + f(i_1 + i_2))$, we must have $f(i_1 + i_2) = f(i_1) + f(i_2)$.

[2] We use $D[x, y]$ to denote the distance between the two words x and y.

Corollary 2.3. *For G to be a linear code, it is necessary that G_2 is a linear code.*

The construction scheme can be varied slightly to yield codes of rate not equal to $\frac{1}{2}$. Let G_1 be an (n, q^k) linear code of distance d_1. Let G_2 be an (n, M_2) code of distance d_2. We consider now two cases.

Case 1. For the case $M_2 < q^{n-k}$, let us select arbitrarily M_2 of the cosets of G_1 and assign to them distinct codewords of G_2. Let i be an n-digit information word that is in one of the cosets selected. We shall encode i as $(i, i + f(i))$, where $f(i)$ is the code-word of G_2 assigned to the coset containing i. The resultant code is thus a $(2n, M_2 \cdot q^k)$ code whose distance is at least equal to $\min(2d_1, d_2)$. Conditions guaranteeing the linearity of the resultant code are the same as that stated in Theorem 2.2. Consequently, in selecting the M_2 cosets of G_1, it is necessary that the following rules be followed:

(1) If a coset A is selected so should be the coset $\{ca \mid a \in A\}$ for any arbitrary c.

(2) If two cosets A_1 and A_2 are selected so should the coset $\{a_1 + a_2 \mid a_1 \in A_1, a_2 \in A_2\}$.

Case 2. For the case $M_2 > q^{n-k}$, let us assume that M_2 is a multiple of q^{n-k}. To be specific, let $M_2 = rq^{n-k}$ for some integer r. We assign to each of the cosets of G_1, r distinct codewords of G_2. Moreover, let R denote a set of r distinct q-ary words. Let there be a one-to-one correspondence between the words in R and the words assigned to each coset of G_1. Let (i_1, i_2) be an information word where i_1 is an n-digit q-ary word, i_2 is a word in R. Such an information word will be encoded as $(i_1, i_1 + f(i_1, i_2))$ where $f(i_1, i_2)$ denotes the word in G_2 that is assigned to the coset containing i_1 and is in correspondence with the word i_2. The resultant code is thus a $(2n, rq^n)$ code. Again, its distance is at least equal to $\min(2d_1, d_2)$. Linearity of the resultant code is guaranteed, if the following conditions are satisfied:

(1) If B is the set of words assigned to the coset containing i, then $\{cb \mid b \in B\}$ must be the set of words assigned to the coset containing ci.

(2) If B_1 is the set of words assigned to the coset containing i_1, B_2 is the set of words assigned to the coset containing i_2, then

$\{b_1 + b_2 \mid b_1 \in B, b_2 \in B_2\}$ must be the set of words assigned to the coset containing $i_1 + i_2$.

3. Linearity of the constituent code G_1

A closer look at the construction scheme presented in Section 2 reveals that linearity of the constituent code G_1 is not a strictly necessary property. What we need in the construction scheme is only a way of partitioning all q-ary ordered n-tuples into disjoint subsets such that the distance between any two ordered n-tuples in the same subset is at least d_1. We illustrate in this section that a systematic code G_1, either linear or non-linear, will also induce one such partition in a natural manner. Without loss of generality, let G_1 be an (n, q^k) systematic code such that the first k digits of the codewords in G_1 are all the distinct q-ary ordered k-tuples. Let $a_1, a_2, \ldots$ denote all ordered n-tuples of the form $(0^k, b)$ where b is an ordered $(n-k)$-tuple. In other words, $a_1, a_2, \ldots$ are ordered n-tuples with k leading zeros. Let

$$U(a) = \{a + g \mid g \in G_1\} .$$

Theorem 3.1. *The set of all ordered n-tuples is partitioned into q^{n-k} disjoint subsets $U(a_1), U(a_2), \ldots$ corresponding to the q^{n-k} ordered n-tuples $a_1, a_2, \ldots$. Moreover, the distance between any two words in a subset $U(a_i)$ is at least d_1.*

Proof. Since $a_i + g_u \neq a_i + g_v$ for distinct g_u and g_v in G_1, we note that every subset $U(a_i)$ contains exactly q^k distinct ordered n-tuples. Moreover, we show that $a_i + g_u \neq a_j + g_v$ for distinct a_i and a_j. If $g_u = g_v$, clearly $a_i + g_u \neq a_j + g_v$. If $g_u \neq g_v$, the first k-digits in g_u must be different from the first k-digits in g_v. Since the first k digits in both a_i and a_j are all zeros, the first k digits in $a_i + g_u$ must be different from the first k digits in $a_j + g_v$. Therefore, $a_i + g_u \neq a_j + g_v$.

For any two words $a_i + g_u$ and $a_i + g_v$ in $U(a_i)$, their distance is equal to $D[g_u, g_v]$ which is at least d_1.

Thus, we can construct a $(2n, q^n)$ code G by assigning the codewords in G_2 to the subsets $U(a_1)$, $U(a_2)$, ..., when the construction scheme in Section 2 is employed. We shall use $f(a_i)$ to denote the codeword in G_2 that is assigned to the subset $U(a_i)$. We have the following theorem concerning the linearity of the code G.

Theorem 3.2. *For G to be a linear code, G_1 must either be a linear code or be a coset of a linear code.*

Proof. Suppose that G is linear. According to Corollary 2.3, G_2 must be a linear code. Thus, G_2 contains the all zero word 0. Let $U(a_i)$ denote the subset of ordered n-tuples to which the all zero word **0** is assigned. Let g_u and g_v be words in G_1. Consider the two words

$$(g_u + a_i, g_u + a_i + f(a_i)) = (g_u + a_i, g_u + a_i),$$
$$(g_v + a_i, g_v + a_i + f(a_i)) = (g_v + a_i, g_v + a_i)$$

in G. Since G is linear, for any constants c_1, c_2,

$$c_1(g_u + a_i, g_u + a_i) + c_2(g_v + a_i, g_v + a_i)$$
$$= (c_1 g_u + c_2 g_v + (c_1 + c_2)a_i,\ c_1 g_u + c_2 g_v + (c_1 + c_2)a_i)$$

is also a word in G. That is, the word

$$(c_1 g_u + c_2 g_v + (c_1 + c_2)a_i,\ c_1 g_u + c_2 g_v + (c_1 + c_2)a_i)$$

can be written as $(g_w + a_j, g_w + a_j + f(a_j))$ for some g_w and a_j. However, $f(a_j)$ is equal to 0 in this case. Thus, $c_1 g_u + c_2 g_v + (c_1 + c_2)a_i$ must be in $U(a_i)$. In other words, for any $g_u + a_i$ and $g_v + a_i$ in $U(a_i)$, $c_1(g_u + a_i) + c_2(g_v + a_i)$ is also in $U(a_i)$. It follows that G_1 is either a linear code (if $a_i = 0$) or a coset of a linear code (if $a_i \neq 0$).

4 Construction examples

In this section we shall present some examples of codes that can be generated by the scheme proposed in the preceding sections.

We show first the construction of an $(8, 2^4, 4)$ binary code. Let G_1 be the $(4, 2^3, 2)$ binary code consisting of all words of even weight. Let G_2 be the $(4, 2, 4)$ binary code consisting of the two words 0000 and 1111. If we assign the word 0000 to the set of code-words in G_1 and assign the word 1111 to the coset of G_1 consisting of all words of odd weight, the resultant code G consists of the words in the following list:

(0000,0000 + 0000) = 00000000,
(0011,0011 + 0000) = 00110011,
(0101,0101 + 0000) = 01010101,
(0110,0110 + 0000) = 01100110,
(1001,1001 + 0000) = 10011001,
(1010,1010 + 0000) = 10101010,
(1100,1100 + 0000) = 11001100,
(1111,1111 + 0000) = 11111111,
(0001,0001 + 1111) = 0011110,
(0010,0010 + 1111) = 00101101,
(0100,0100 + 1111) = 01001011,
(0111,0111 + 1111) = 01111000,
(1000,1000 + 1111) = 10000111,
(1011,1011 + 1111) = 10110100,
(1101,1101 + 1111) = 11010010,
(1110,1110 + 1111) = 11100001.

As a matter of fact, we can construct a class of linear and non-linear binary codes that have the same parameters (block length, number of codewords and distance) as the Reed–Muller codes. We shall show the construction of codes of block length 2^m, distance 2^{m-r} which has 2^k codewords where

$$k = 1 + \binom{m}{1} + \binom{m}{2} + \dots + \binom{m}{r}.$$

(Clearly, these are the parameters of an r^{th} order Reed–Muller code of block length 2^m.) Let G_1 be an r^{th} order Reed–Muller code of block length 2^{m-1}. The distance of G_1 is 2^{m-r-1}. The number of codewords in G_1 is 2^{k_1} where

$$k_1 = 1 + \binom{m-1}{1} + \binom{m-1}{2} + \ldots + \binom{m-1}{r} .$$

The number of cosets of G_1 is 2^{m-k_1-1}. Let G_2 be an $(r-1)^{st}$ order Reed–Muller code of block length 2^{m-1}. The distance of G_2 is 2^{m-r}. The number of codewords in G_2 is 2^{k_2} where

$$k_2 = 1 + \binom{m-1}{1} + \binom{m-1}{2} + \ldots + \binom{m-1}{r-1} .$$

If we assign $2^{k_2-(m-k_1-1)}$ distinct codewords of G_2 to each of the cosets of G_1, the resultant code G is of block length 2^m and distance 2^{m-r}. The number of codewords in G is

$$2^{m-1} \cdot 2^{k_2-(m-k_1-1)} = 2^{k_1+k_2} .$$

However, since

$$k_1 + k_2 = 1 + \binom{m}{1} + \binom{m}{2} + \ldots + \binom{m}{r} ,$$

the parameters of G are indeed identical to that of an r^{th} order Reed–Muller code of block length 2^m Note that our construction procedure imposes no restriction on how the codewords of G_2 are assigned to the cosets of G_1. Thus, the possibility of obtaining a class of linear and non-linear codes is quite clear.

We show now the construction of a class of non-linear codes that have the same parameters as a class of codes discovered by Sloane and Whitehead [9]. Again, because of the flexibility in our construction scheme in assigning codewords in G_2 to the cosets of G_1, corresponding to each of the codes discovered by Sloane and Whitehead, there is a class of non-linear codes with the same set of parameters.

Golay [11] and Julin [2] have discovered binary single error correcting codes of block length 8, 9, 10, 11. The parameters of these codes are (8, 20, 3), (9, 38, 3), (10, 72, 3), (11, 144, 3). We shall denote these codes by C_8, C_9, C_{10}, C_{11}, respectively. Let G_1 be an $(8, 2^7, 2)$ single parity check code. Let G_2 be the (8, 20, 3) code C_8. By assigning 10 of the codewords of C_8 to each coset of G_1, we obtain a $(16, 10 \cdot 2^8, 3)$ code. Moreover, different assignments of the codewords of C_8 to the cosets of C_1 yield a whole class of $(16, 10 \cdot 2^8, 3)$ codes. Let G_1 be a

$(9, 2^8, 2)$ single parity check code. Let G_2 be the $(9, 20, 4)$ code obtained by appending a parity check bit to the codewords in C_8. Our construction procedure yields a class of $(18, 10 \cdot 2^9, 4)$ codes which can be shortened to yield a class of $(17, 10 \cdot 2^9, 3)$ codes. Let G_1 be a $(9, 2^8, 2)$ single parity check code. Let G_2 be the $(9, 38, 2)$ code C_9. By assigning 19 of the codewords of G_2 to each coset of G_1, we obtain a class of $(18, 19 \cdot 2^9, 3)$ codes. Again, let G_1 be a $(10, 2^9, 2)$ single parity check code. Let G_2 be the $(10, 38, 4)$ code obtained by appending a parity check bit to the codewords in C_9. We can then construct a class of $(20, 19 \cdot 2^{10}, 4)$ codes which can be shortened to yield a class of $(19, 19 \cdot 2^{10}, 3)$ codes. Similarly, we can construct classes of codes with the following parameters: $(20, 36 \cdot 2^{10}, 3)$, $(21, 36 \cdot 2^{11}, 3)$, $(22, 72 \cdot 2^{11}, 3)(23, 72 \cdot 2^{12}, 3)$.

Furthermore, let G_1 be a $(16, 2^{15}, 2)$ single parity check code. Let G_2 be one of the $(16, 10 \cdot 2^8, 3)$ codes constructed above. We can employ our construction procedure to obtain a class of $(16, 10 \cdot 2^{23}, 3)$ codes. Repeating the construction procedure recursively, we have:

Theorem 4.1. *For any block length n satisfying $2^m \leq n < 3 \cdot 2^{m-1}$, there exists a class of non-linear $(n, \lambda \cdot 2^{n-m-1}, 3)$ codes where $\lambda = \frac{5}{4}, \frac{19}{16}$, or $\frac{9}{8}$ according to the binary expansion of n that begins with* 1000, 1001, or 101 ... .

Theorem 4.1 is an extension of a theorem due to Sloane and Whitehead [9], who employed a construction scheme quite similar to ours (see Section 6). It is not difficult to see that corresponding to each code constructed by the Sloane and Whitehead scheme, our construction yields a class of codes which can be obtained by adding a certain fixed word to half of the words in the code obtained in the Sloane and Whitehead construction. We leave the details to the interested reader.

More construction examples can be found in [8].

5. Construction of a class of optimal non-linear codes

As was pointed out above, $\min(2d_1, d_2)$ is only a lower bound to the distance of the constructed according to our scheme. Indeed, we shall show in this section the construction of a class of non-linear codes whose distances exceed the lower bound $\min(2d_1, d_2)$. Intuitively, such a possibility does not come in as a surprise. Since our construction scheme allows complete freedom in assigning words of G_2 to cosets of G_1, one would suspect that the distance of the resultant code G might be improved if a judicious assignment is made.

We begin with the construction of a $(16, 2^8, 6)$ binary code which is the extended $(15, 2^8, 5)$ code discovered by Robinson and Nordstrom [4; 6]. Let both G_1 and G_2 be the $(8, 2^4, 4)$ binary code obtained by appending a parity check bit to the $(7, 2^4, 3)$ cyclic code generated by the polynomial $1 + x + x^3$. Any casual assignment of the 16 words in G_2 to the 16 cosets of G_1 will yield a code of distance 4. However, let us examine the assignment in Table 2, where the cosets of G_1 are identified by the coset leaders. (Since the distance of G_1 is 4, the coset leaders in Table 2 are leaders of distinct cosets.) We show now that such an assignment yields a code of distance 6.

Table 2

Cosets of G_1 (identified by their leaders)	Assignment of words in G_2 to the cosets
00000000	00000000
10000000	00010111
01000000	10001011
00100000	11000101
00010000	01100011
00001000	10110001
00000100	01011001
00000010	00101101
00000001	11111111
10000001	11101000
01000001	01110100
00100001	00111010
00010001	10011100
00001001	01001110
00000101	10100110
00000011	11010010

We introduce first some notation. Let x, y be two binary ordered n-tuples. We shall use $|x|$ to denote the (Hamming) weight of x, and xy to denote the ordered n-tuple obtained by componentwise multiplication of x and y. It is easy to check that

$$|x| + |y| = |x + y| + 2|xy| .$$

Moreover, we also have

$$(5.1) \qquad \begin{aligned} |x+y| + |x+y+z| &= |z| + 2|(x+y)(x+y+z)| \\ &= |z| + 2|(x+y) + (x+y)z| \\ &= |z| + 2|x(x+z) + y(y+z)| . \end{aligned}$$

Let $l_1, l_2, \ldots$ denote the cosets leaders of G_1, and $f(l_1), f(l_2), \ldots$ denote the words assigned to them as shown in Table 2. It can be verified directly that

$$|(l_1 + l_2)(l_1 + l_2 + f(l_1) + f(l_2))| = 1$$

if $|f(l_1) + f(l_2)| = 4$.

We are now ready to prove that the distance of the code G is equal to 6. Let $(i_1, i_1 + f(i_1))$ and $(i_2, i_2 + f(i_2))$ be two codewords in G. The distance between these two words is

$$|i_1 + i_2, i_1 + i_2 + f(i_1) + f(i_2)| .$$

Since $i_1 = l_1 + m_1$, $i_2 = l_2 + m_2$, where m_1 and m_2 denote codewords in G_1, according to (5.1), the distance can also be written as

$$\begin{aligned} &|l_1 + m_1 + l_2 + m_2, l_1 + m_1 + l_2 + m_2 + f(l_1) + f(l_2)| \\ &\quad = |f(l_1) + f(l_2)| + 2|(l_1 + l_2)(l_1 + l_2 + f(l_1) + f(l_2)) \\ &\qquad + (m_1 + m_2)(m_1 + m_2 + f(l_1) + f(l_2))|. \end{aligned}$$

We examine three cases:

Case 1. $|f(l_1) + f(l_2)| = 8$. Clearly, the distance between the two words is larger than or equal to 8.

Case 2. $|f(l_1) + f(l_2)| = 0$. This implies that $l_1 = l_2$ and $f(l_1) = f(l_2)$. The distance of the two words is then

$$2|(m_1 + m_2)(m_1 + m_2)| = 2|(m_1 + m_2)| \geq 8$$

because $m_1 \neq m_2$.

Case 3 $|f(l_1)+f(l_2)| = 4$. As was pointed out above, we have

$$|(l_1 + l_2)(l_1 + l_2 + f(l_1) + f(l_2))| = 1 .$$

Since $m_1, m_2, f(l_1), f(l_2)$ are in G_1, $|(m_1 + m_2)(m_1 + m_2 + f(l_1)+f(l_2))|$ is an even number. It follows that

$$|(l_1 + l_2)(l_1 + l_2 + f(l_1)+f(l_2)) + (m_1+m_2)(m_1+m_2+ f(l_1)+f(l_2))| > 0.$$

The distance of the code is thus at least 6.

Our construction scheme can be applied to construct a class of optimal non-linear codes discovered by Preparata [7]. We outline here the construction steps which are motivated by Preparata's original construction. Let both G_1 and G_2 be the $(m-3)^{\text{rd}}$ order Reed–Muller code of length 2^{m-1} obtained by appending a parity check bit to the cyclic code generated by

$$g(x) = \prod_{j=0}^{m-2} (x-\alpha^{2^j}) , \tag{5.2}$$

where α is a primitive element in $\mathrm{GF}(2^{m-1})$ (see [3]). Thus, both G_1 and G_2 are $(2^{m-1}, 2^{2^{m-1}-m}, 4)$ codes. Consequently, to each of the 2^m cosets of G_1, we shall assign $2^{2^{m-1}-2m}$ codewords in G_2. Although any arbitrary assignment will yield a $(2^m, 2^{2^m-2m})$ code of distance 4, the assignment shown below will increase the distance to 6.

In order to obtain a resultant code of distance 6, we must assign to each coset of G_1 words of mutual distance at least equal to 6. Let S denote the cyclic code of length $2^{m-1}-1$ whose generator polynomial has $1, \alpha, \alpha^3$ as its roots. Clearly, S is a BCH code of distance 6. Note that S is a subcode of the cyclic code generated by $g(x)$ in (5.2). By appending a parity check bit to the words in S, we obtain a subcode of G_2 whose distance is 6. Call this subcode of G_2, S'. It can be shown that S' has $2^{2^{m-1}-2m}$ codewords when m is even (see [5]). We now assign the words in the cosets of S' (with respect to G_2) to the cosets of G_1 as shown in Table 3 where the cosets of G_1 and S' are identified by their coset leaders. (It is not difficult to show that these are leaders of distinct cosets.) In Table 3, we use the standard polynomial notation for ordered 2^m-tuples.

Table 3

Cosets of G_1	Cosets of S'
0	0
1	$(f(x)+1)+x^{2^{m-1}-1}$
x	$x(f(x)+1)+x^{2^{m-1}-1}$
x^2	$x^2(f(x)+1)+x^{2^{m-1}-1}$
$\vdots$	$\vdots$
$x^{2^{m-1}-2}$	$x^{2^{m-1}-2}(f(x)+1)+x^{2^{m-1}-1}$
$x^{2^{m-1}-1}$	$x^{2^{m-1}-1}+u(x)$
$1+x^{2^{m-1}-1}$	$(f(x)+1)+x^{2^{m-1}-1}+u(x)$
$x+x^{2^{m-1}-1}$	$x(f(x)+1)+x^{2^{m-1}-1}+u(x)$
$x^2+x^{2^{m-1}-1}$	$x^2(f(x)+1)+x^{2^{m-1}-1}+u(x)$
$\vdots$	$\vdots$
$x^{2^{m-1}-2}+x^{2^{m-1}-1}$	$x^{2^{m-1}-2}(f(x)+1)+x^{2^{m-1}-1}+u(x)$

In Table 3, $f(x)$ is the polynomial $x^t h(x)$, where

$$h(x) = (x^{2^{m-1}-1} + 1)/g(x)$$

and t is an integer such that

$$h^2(x) = x^{2^{m-1}-1-t}h(x).$$

Also, $u(x)$ is the polynomial

$$1 + x + x^2 + x^3 + \dots + x^{2^{m-1}-1}$$

corresponding to the ordered 2^{m-1}-tuple of all 1's.

We shall not include a proof of the distance of the resultant code here (see [5]). Moreover, it is also not difficult to see the relationship between Preparata's construction and our construction and thus to invoke Preparata's results to support the claim.

6. Remarks

Our construction scheme bears a close resemblance to that of Sloane and Whitehead [9]. As a matter of fact, the Sloane and Whitehead scheme can be viewed as a special case of our scheme in which only one coset of G_1 (G_1 itself) is used and to this coset all words of G_2 are assigned. It should be pointed out that our construction scheme can generate non-linear codes from linear constituent codes while the Sloane and Whitehead scheme generates only linear codes from linear constituent codes. Also, it is possible in our construction scheme to attain a distance better than $\min(2d_1, d_2)$; yet in the Sloane and Whitehead scheme, $\min(2d_1, d_2)$ is always the distance of the resultant code. Unfortunately, very little is known at this moment about the assignment of codewords of G_2 to cosets of G_1 so that a distance larger than $\min(2d_1, d_2)$ can be attained.

References

[1] M.J.E. Golay, Binary coding, IEEE Trans. Inform. Theory PGIT–4 (1954) 23–28.

[2] D. Julin, Two improved block codes, IEEE Trans. Inform. Theory IT–11 (1965) 549.

[3] T. Kasami, S. Lin and W.W. Peterson, Reed-Muller codes, part I: Primitive codes, IEEE Trans. Inform. Theory IT–14 (2) (1968) 189–199.

[4] A.E. Nordstrom and J.P. Robinson, An optimum non-linear code, Inform. Control (1967) 613–617.

[5] B.G. Ong, A new construction scheme for linear and non-linear codes, S.M. Thesis, Dept. of Elec. Eng., Massachusetts Inst. of Technol., Cambridge, Mass. (1970).

[6] F.P. Preparata, Weight and distance structure of Nordstrom-Robinson quadratic code, Inform. Control (1968) 466–473.

[7] F.P. Preparata, A class of optimum non-linear double-error-correcting codes, Inform. Control (1968) 378–400.

[8] G.R. Ruth, A new technique for the construction of block codes, S.M. Thesis, Dept. of Elec.Eng., Massachusetts Inst. of Technol., Cambridge, Mass. (1971).

[9] N.J.A. Sloane and D.S. Whitehead, New family of single-error-correcting codes, IEEE Trans. Inform. Theory IT–16 (6) (1970) 717–719.