3.5 The Extended Golay Code

In this and the next two sections we construct and decode two codes which will correct three or fewer errors. The extended Golay code, discussed in this and the next section, was in fact used in the Voyager spacecraft program which, in the early 1980's, brought us those marvelous close-up photographs of Jupiter and Saturn.

Let B be the 12×12 matrix

$$B = \begin{bmatrix} 1&1&0&1&1&1&0&0&0&1&0&1 \\ 1&0&1&1&1&0&0&0&1&0&1&1 \\ 0&1&1&1&0&0&0&1&0&1&1&1 \\ 1&1&1&0&0&0&1&0&1&1&0&1 \\ 1&1&0&0&0&1&0&1&1&0&1&1 \\ 1&0&0&0&1&0&1&1&0&1&1&1 \\ 0&0&0&1&0&1&1&0&1&1&1&1 \\ 0&0&1&0&1&1&0&1&1&1&1&0 \\ 0&1&0&1&1&0&1&1&1&0&0&1 \\ 1&0&1&1&0&1&1&1&0&0&0&1 \\ 0&1&1&0&1&1&1&0&0&0&1&1 \\ 1&1&1&1&1&1&1&1&1&1&1&0 \end{bmatrix}.$$

Let G be the 12×24 matrix $G = [I, B]$, where I is the 12×12 identity matrix. The linear code C with generator matrix G is called the *extended Golay code* and will be denoted by C_{24}.

As an aid to remembering B, note that the 11×11 matrix B_1 obtained from B by deleting the last row and column has a cyclic structure. The first row of B_1 is 11011100010. The second row is obtained from the first by shifting each digit one position to the left and moving the first digit to the end. The third row is obtained from the second row in the same way, and so on for the remaining rows. Thus B may be remembered as the matrix

$$B = \begin{bmatrix} B_1 & j^T \\ j & 0 \end{bmatrix},$$

where j is the word of all ones of length 11. By inspection, we see that $B^T = B$; that is, B is a symmetric matrix.

We now list seven important facts about the extended Golay code C_{24} with generator matrix $G = [I, B]$:

(1) C_{24} has length $n = 24$, dimension $k = 12$ and $2^{12} = 4096$ codewords. This is clear upon inspection of G.

(2) A parity check matrix for C_{24} is the 24×12 matrix

$$\begin{bmatrix} B \\ I \end{bmatrix}$$

Algorithm 2.5.7 yields this fact.

(3) Another parity check matrix for C_{24} is the 24×12 matrix

$$H = \begin{bmatrix} I \\ B \end{bmatrix}.$$

To see this, note first that each row of B has odd weight (7 or 11). The scalar (dot) product of any row with itself is therefore 1. Next, a manual check shows that the scalar product of the first row of B with any other row is 0. From the cyclic structure of B_1 it follows that the scalar product of any two different rows of B is 0. Thus $BB^T = I$. But $B^T = B$, so $B^2 = BB^T$ and,

$$GH = [I, B] \begin{bmatrix} I \\ B \end{bmatrix} = I^2 + B^2 = I + BB^T = I + I = 0.$$

We shall use both parity check matrices to decode C_{24}.

(4) Another generator matrix for C_{24} is the 12×24 matrix $[B, I]$.

(5) C_{24} is self-dual; that is, $C_{24} = C_{24}^{\perp}$.

(6) The distance of C is 8.

(7) C_{24} is a three-error-correcting code.

The proofs of facts (4) and (5) are requested in exercises. We will give a proof of fact (6) which, in the bargain, contains further useful information about the code C_{24}. The proof is divided into three stages:

Stage I. The weight of any word in C_{24} is a multiple of 4. To see this, note first that the rows of G have weight 8 or 12. Let v be a word in C_{24} which is the sum $v = r_i + r_j$ of two different rows of G. The rows of B are orthogonal; hence the rows of G are orthogonal. Therefore r_i and r_j have an even number, say $2x$, of ones in common. Thus

$$wt(v) = wt(r_i) + wt(r_j) - 2(2x)$$

is a multiple of 4.

Now suppose the word v in C_{24} is the sum $v = r_i + r_j + r_k$ of three different rows of G. Let $v_1 = r_i + r_j$. Since C_{24} is self-dual, v_1 and r_k have scalar product 0, and hence an even numer, say $2y$, of ones in common. Thus

$$wt(v) = wt(v_1) + wt(r_k) - 2(2y)$$

is a multiple of 4. Continuing in this vein (formally, by induction) we see that if v in C_{24} is a linear combination of rows of G, then $wt(v)$ must be a multiple of 4.

Stage II. The first eleven rows of G are codewords in C_{24} of weight 8, so the distance of C_{24} must be either 4 or 8.

Stage III. We rule out words of weight 4 being codewords in C_{24}. Let v be a nonzero codeword in C_{24}, and suppose $wt(v) = 4$. Then $v = u_1[I, B]$ and $v = u_2[B, I]$ for some u_1 and u_2 (since both $[I, B]$ and $[B, I]$ generate C_{24}) and $wt(u_1) \leq 2$ or $wt(u_2) \leq 2$ (since one half of v must contain at most two 1's). However no sum of one or two row of B has weight at most 3, so $wt(v) = wt(u_i) + wt(u_iB) > 4$. Therefore v does not have weight 4.

□

Exercises

3.5.1 Show that the word of all ones is in C_{24}. Deduce that C_{24} contains no words of weight 20.

3.5.2 Prove fact (4) about C_{24}.

3.5.3 Prove fact (5) about C_{24}.

3.5.4 Use Theorem 2.9.1 to verity that C_{24} has distance 8.

3.6 Decoding the Extended Golay Code

We shall now find an algorithm for IMLD for the code C_{24}. Throughout this section, w denotes the word received, v the closest codeword to w and u the error pattern $v + w$. For C_{24} we want to correct all error patterns of weight at most 3, so we assume that $wt(u) \leq 3$. A comma will be placed between the first 12 and the last 12 digits of words in K^{24}. The error pattern u will be denoted by $[u_1, u_2]$, where u_1 and u_2 each have length 12. Our aim is to determine the coset leader, u of the coset containing w without having to refer to the SDA of C_{24}

Since we are assuming that $wt(u) \leq 3$, either $wt(u_1) \leq 1$ or $wt(u_2) \leq 1$. Let s_1 be the syndrome of $w = v + u$ using the parity check matrix

$$H = \begin{bmatrix} I \\ B \end{bmatrix}.$$

Then $s_1 = wH = [u_1, u_2]H = u_1 + u_2B$. So if $wt(u_2) \leq 1$ then s_1 consists of either a word of weight at most 3 (if $wt(u_2) = 0$) or a row of B with at most 2 of its digits changed (if $wt(u_2) = 1$). Similary, if $wt(u_1) \leq 1$ then the syndrome

$$s_2 = w \begin{bmatrix} B \\ I \end{bmatrix} = u_1B + u_2$$

consists of either a word of weight at most 3 or a row of B with at most 2 of its digits changed.

In any case, if u has weight at most 3 then it is easily identified, since at most 3 rows of one of the two parity check matrices can be found to add to the corresponding syndrome. Using this observation we obtain the following decoding algorithm. We shall make use of the fact that $B^2 = I$ and

$$\begin{aligned} s_1 &= u_1 + u_2B = wH \\ s_2 &= u_1B + u_2 \\ &= (u_1 + u_2B)B = s_1B. \end{aligned}$$

To avoid incorporating both of the parity check matrices into the algorithm, only $H = \begin{bmatrix} I \\ B \end{bmatrix}$ is used. Of course once u has been determined, w is decoded to the codeword $v = w + u$. e_i is the word of length 12 with a 1 in the ith position and $0's$ elsewhere, and b_i is the i^{th} row of B.

Algorithm 3.6.1 (IMLD for C_{24}).

1. Compute the syndrome $s = wH$.
2. If $wt(s) \leq 3$ then $u = [s, 0]$.
3. If $wt(s + b_i) \leq 2$ for some row b_i of B then $u = [s + b_i, e_i]$.
4. Compute the second syndrome sB.
5. If $wt(sB) \leq 3$ then $u = [0, sB]$.
6. If $wt(sB + b_i) \leq 2$ for some row b_i of B then $u = [e_i, sB + b_i]$.
7. If u is not yet determined then request retransmission.

The above algorithm requires at most 26 weight calculations in the decoding procedure. (Of course, once u has been determined then no further steps in the algorithm need to be done.)

Example 3.6.2 Decode $w = 101111101111, 010010010010$. The syndrome is

$$\begin{aligned} s = wH &= 101111101111 + 001111101110 \\ &= 100000000001, \end{aligned}$$

which has weight 2. Since $wt(s) \leq 3$, we find that

$$u = [s, 0] = 100000000001, 000000000000$$

and conclude that

$$v = w + u = 001111101110, 010010010010$$

was the codeword sent.

Because $G = [I, B]$ is in standard form and any word in K^{12} can be encoded as a message (C_{24} has dimension 12), the message sent appears in the first 12 digits of the decoded word v. In Example 3.6.2 the message 001111101110 was sent.

Example 3.6.3 Decode $w = 001001001101, 101000101000$. The syndrome is

$$s = wH = 001001001101 + 111000000100 = 110001001001,$$

which has weight 5. Proceeding to step 3 of the Algorithm 3.6.1 we compute

$$\begin{aligned} s + b_1 &= 000110001100 \\ s + b_2 &= 011111000010 \\ s + b_2 &= 101101011110 \\ s + b_4 &= 001001100100 \\ s + b_5 &= 000000010010. \end{aligned}$$

Since $wt(s + b_5) \leq 2$, we find that

$$u = [s + b_5, e_5] = 000000010010, 000010000000$$

and conclude that

$$v = w + u = 001001011111, 101010101000$$

was the codeword sent.

Example 3.6.4 Decode $w = 000111000111, 011011010000$. The syndrome is

$$\begin{aligned} s = wH &= u_1 + u_2 B \\ &= 000111000111 + 101010101101 \\ &= 101101101010, \end{aligned}$$

which has weight 7. Proceeding to step 3, we find $wt(s + b_i) \geq 3$ for each row b_i of B. We continue to step 4; the second syndrome is

$$sB = 111001111101,$$

which has weight 9. Forging ahead to step 5 we compute

$$\begin{aligned} sB + b_1 &= 001110111000 \\ sB + b_2 &= 010111110110 \\ sB + b_3 &= 100101101010 \\ sB + b_4 &= 000001010000. \end{aligned}$$

Since $wt(sB + b_4) \leq 2$, we find that

$$u = [e_4, sB + b_4] = 000100000000, 000001010000$$

and conclude that

$$v = w + u = 000011000111, 011010000000$$

was the codeword sent.

Exercises

3.6.5 The code is C_{24}. Decode, if possible, each of the following received words w.

(a) 111 000 000 000, 011 011 011 011
(b) 111 111 000 000, 100 011 100 111
(c) 111 111 000 000, 101 011 100 111
(d) 111 111 000 000, 111 000 111 000
(e) 111 000 000 000, 110 111 001 101
(f) 110 111 001 101, 111 000 000 000
(g) 000 111 000 111, 101 000 101 101
(h) 110 000 000 000, 101 100 100 000
(i) 110 101 011 101, 111 000 000 000.

3.6.6 Find the most likely error pattern for any word with the given syndromes.

(a) $s_1 = 010010000000$, $s_2 = 011111010000$
(b) $s_1 = 010010100101$, $s_2 = 001000110000$
(c) $s_1 = 111111000101$, $s_2 = 111100010111$
(d) $s_1 = 111111111011$, $s_2 = 010010001110$
(e) $s_1 = 001101110110$, $s_2 = 111110101101$
(f) $s_1 = 010111111001$, $s_2 = 100010111111$.

3.6.7 Show that if s or sB has weight 4 then IMLD requires that the word be retransmitted.

3.7 The Golay Code

Another interesting three-error-correcting code can be obtained by *puncturing* C_{24}, that is, by removing a digit from every word in C_{24}. The same digit must be removed from each word. We shall remove the last digit.

Let $\hat{B}$ be the 12×11 matrix obtained from the matrix B by deleting the last column. Let G be the 12×23 matrix $G = [I_{12}, \hat{B}]$. The linear code with generator matrix G is called the Golay code and is denoted by C_{23}. The Golay code has length $n = 23$, dimension $k = 12$, and contains $2^{12} = 4096$ codewords. Note that the extended code C_{23}^* is indeed C_{24}. C_{23} has distance 7. This is most easily seen from the fact that $C_{23}^* = C_{24}$ (see Exercise 3.4.6), but can be shown using Theorem 3.2.8 or by modifying the proof that C_{24} has distance 8.

The Golay code C_{23} is a perfect code (Example 3.2.4) *and will correct all error patterns of weight 3 or less, and no others* (Theorem 3.2.8). Therefore

every received word w is at most distance 3 from exactly one codeword. So if we append the digit 0 or 1 to w forming $w0$ or $w1$ respectively so that the resulting word has odd weight, then the resulting word is distance at most 3 from a codeword c in C_{24} (see Exercise 3.7.8). Decoding to c using Algorithm 3.6.1 and removing the last digit from c then gives the closest codeword to w in C_{23}.

Algorithm 3.7.1 (Decoding algorithm for the Golay Code.)

1. Form $w0$ or $w1$, whichever has odd weight.
2. Decode wi (i is 0 or 1) using Algorithm 3.6.1 to a codeword c in C_{24}.
3. Remove the last digit from c.

In practice, the received word w is normally a codeword, however wi formed in step 1 is never a codeword (Why?). If w is a codeword then the syndrome of wi is the last row of H (Why?) so this can easily be checked before implementing Algorithm 3.6.1

Example 3.7.2 Decode $w = 001001001001, 11111110000$. Since w has odd weight, form $w0 = 001001001001, 111111100000$. Then $s_1 = 100010111110$. Since $s_1 = b_6 + e_9 + e_{12}, w0$ is decoded to $001001000000, 111110100000$ and so w is decoded to $001001000000, 11111010000$.

Exercises

3.7.3 Decode each of the following received words that were encoded using C_{23}.

(a) 101011100000, 10101011011

(b) 101010000001, 11011100010

(c) 100101011000, 11100010000

(d) 011001001001, 01101101111.

3.7.4 Prove that C_{23} has distance $d = 7$.

3.7.5 Find the reliability of C_{23} transmitted over a BSC of probability p.

3.7.6 Determine whether C_{23} or C_{24} has the greater reliability. Use the same BSC for both.

3.7.7 Use the fact that every word of weight 4 is distance 3 from exactly one codeword (why?) to count the number of codewords of weight 7 in the Golay Code (Hint: for any codeword c, the number of words that have weight 4 and are distance 3 from c is $\binom{7}{3}$).

3.7.8 Use Exercise 3.7.7 to show that C_{24} contains precisely 759 codewords of weight 8.

3.7.9 Use Exercises 3.5.1 and 3.7.8 to verify the following weight distribution table for C_{24}:

weight	0	4	8	12	16	20	24
number of words	1	0	759	2576	759	0	1

3.7.10 Let w be a received word that was encoded using C_{23}. Append a digit i to w to form a word wi of odd weight. Show that wi is within distance 3 of a codeword in C_{24}. (Hint: all words in C_{24} have even weight.)

3.8 Reed-Muller Codes

In this section we consider another important class of codes which includes the extended Hamming code discussed earlier. The r^{th} order Reed-Muller code of length 2^m will be denoted by $RM(r,m), 0 \leq r \leq m$. We present a recursive definition of these codes

(1) $RM(0,m) = \{00\ldots0, 11\ldots1\}, RM(m,m) = K^{2^m}$

(2) $RM(r,m) = \{(x, x+y) | x \in RM(r,m-1), y \in RM(r-1,m-1)\}, 0 < r < m$.

So $RM(m,m)$ is all words of length 2^m and $RM(0,m)$ is just the all ones word (and the zero word).

Example 3.8.1

$$\begin{array}{ll} RM(0,0) = \{0,1\} & \\ RM(0,1) = \{00,11\}, & RM(1,1) = K^2 = \{00,01,10,11\} \\ RM(0,2) = \{0000,1111\}, & RM(2,2) = K^4 \\ RM(1,2) = \{(x,x+y) | & x \in \{00,01,10,11\}, y \in \{00,11\}\} \end{array}$$

Rather than use this description of the code, we will give a recursive construction for the generator matrix of $RM(r,m)$, which we will denote by $G(r,m)$. For $0 < r < m$, define $G(r,m)$ by

$$G(r,m) = \begin{bmatrix} G(r,m-1) & G(r,m-1) \\ 0 & G(r-1,m-1) \end{bmatrix}$$

For $r = 0$ define

$$G(0,m) = [11\ldots1]$$

and for $r = m$, define

$$G(m,m) = \begin{bmatrix} G(m-1,m) \\ 0\ldots01 \end{bmatrix}$$