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~~10). 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

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

Example 3.8.2 The generator matrices for $RM(0,1)$ and $RM(1,1)$ are

$$G(0,1) = (1\ 1) \text{ and } G(1,1) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

Example 3.8.3 Let $m = 2$, then the length is $4 = 2^2$ and for $r = 1,2$ we have

$$G(1,2) = \begin{bmatrix} G(1,1) & G(1,1) \\ 0 & G(0,1) \end{bmatrix}, G(2,2) = \begin{bmatrix} G(1,2) \\ 0001 \end{bmatrix}.$$

Using Example 3.8.2 we have,

$$G(1,2) = \begin{bmatrix} 11 & 11 \\ 01 & 01 \\ 00 & 11 \end{bmatrix}, G(2,2) = \begin{bmatrix} 1111 \\ 0101 \\ 0011 \\ 0001 \end{bmatrix}$$

Example 3.8.4 For $m = 3, m = 2^3 = 8$, we have

$$G(0,3) = (11111111), G(3,3) = \begin{bmatrix} G(2,3) \\ 00000001 \end{bmatrix}$$

$$G(1,3) = \begin{bmatrix} G(1,2) & G(1,2) \\ 0 & G(0,2) \end{bmatrix}, G(2,3) = \begin{bmatrix} G(2,2) & G(2,2) \\ 0 & G(1,2) \end{bmatrix}.$$

Thus using Example 3.8.3

$$G(1,3) = \begin{bmatrix} 1111 & 1111 \\ 0101 & 0101 \\ 0011 & 0011 \\ 0000 & 1111 \end{bmatrix}$$

Exercises

3.8.5 Find the generator matrix $G(2,3)$.

3.8.6 Find generator matrix $G(r,4)$, for the codes $RM(r,4)$ for $r = 0,1,2$.

With this recursive definition it is a simple matter to prove via induction the basic properties of a Reed-Muller code.

Theorem 3.8.7 *The r^{th} order Reed-Muller code $RM(r,m)$ defined above has the following properties:*

(1) length $n = 2^m$

(2) distance $d = 2^{m-r}$

(3) dimension $k = \sum_{i=0}^{r} \binom{m}{i}$

(4) $RM(r-1,m)$ is contained in $RM(r,m), r > 0$

(5) dual code $RM(m-1-r,m), r < m$.

Proof: The proofs of these claims all use induction. We leave it as an exercise to show that this theorem holds for all $RM(r,m)$ codes for $m = 1,2,3,4$. Also, we note that these claims are obviously true for $r = 0$ and $r = m$.

First we want to show that $RM(r-1,m) \subseteq RM(r,m)$. We start with,

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

Since $\mathbf{1}$ is the top row of $G(1,m-1)$ then the all ones vector $(\mathbf{1},\ \mathbf{1})$ is the top row vector in $(G(1,m-1), G(1,m-1))$. Thus $RM(0,m) = \{\mathbf{0},\ \mathbf{1}\}$ is contained in $RM(1,m)$.

In general since $G(r-1,m-1)$ is a submatrix of $G(r,m-1)$ and $G(r-2,m-1)$ is a submatrix of $G(r-1,m-1)$ we have obviously the

$$G(r-1,m) = \begin{pmatrix} G(r-1,m-1) & (G(r-1,m-1) \\ 0 & G(r-2,m) \end{pmatrix}$$

is a submatrix of $G(r,m)$ and thus $RM(r-1,m)$ is a subcode of $RM(r,m)$.

Next we establish the distance $d = 2^{m-r}$ for $RM(r,m)$, using induction on r.

Since $RM(r,m) = \{(x, x+y) | x \in RM(r,m-1), y \in RM(r-1,m-1)\}$ and $RM(r-1,m-1) \subseteq RM(r,m-1)$ then $x+y \in RM(r,m-1)$ and so if $x \neq y$, then, by our inductive hypothesis, $wt(x+y) \geq 2^{m-1-r}$. Also $wt(x) \geq 2^{m-1-r}$. Hence $wt(x,x+y) = wt(x+y) + wt(x) \geq 2 \cdot 2^{m-1-r} = 2^{m-r}$. If $x = y$, then $(x, x+y) = (y, 0)$ but $y \in RM(r-1,m-1)$ and thus $wt(y,0) = wt(y) \geq 2^{m-1-(r-1)} = 2^{m-r}$.

From the definition of $G(r,m)$, we have

$$\begin{aligned} \dim RM(r,m) &= \dim RM(r,m-1) + \dim RM(r-1,m-1) \\ &= \sum_{i=0}^{r} \binom{m-1}{i} + \sum_{i=0}^{r-1} \binom{m-1}{i} \\ &= \sum_{i=1}^{r} \left(\binom{m-1}{i} + \binom{m-1}{i-1} \right) + \binom{m-1}{0}. \end{aligned}$$

Since $\binom{m}{i} = \binom{m-1}{i} + \binom{m-1}{i-1}$ and $\binom{m-1}{0} = 1 = \binom{m}{0}$ we have,

$$\dim RM(r,m) = \sum_{i=0}^{r} \binom{m}{i}.$$

Finally let

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

and let

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

By induction the dual of $RM(r, m-1)$ is $RM(m-r-2, m-1)$ and the dual of $RM(r-1, m-1)$ is $RM(m-r-1, m-1)$ thus $x \cdot y' = 0$, and $x' \cdot y = 0$. Also since $RM(r-1, m-1) \subseteq RM(r, m-1)$, $y \cdot y' = 0$. Hence

$$\begin{aligned}(x, x+y) \cdot (x', x'+y') &= (x+y) \cdot (x'+y') + x \cdot x' \\ &= 2(x \cdot x') + x \cdot y' + y \cdot x' + y \cdot y' \\ &= 0.\end{aligned}$$

We see that every vector in $RM(r,m)$ is orthogonal to every vector in $RM(m-r-1, m)$. Since

$$\begin{aligned}\dim RM(r,m) + \dim RM(m-r-1,m) &= \sum_{i=0}^{r} \binom{m}{i} + \sum_{i=0}^{m-r-1} \binom{m}{i} \\ &= \sum_{i=0}^{r} \binom{m}{m-i} + \sum_{j=0}^{m-r-1} \binom{m}{j} \\ &= \sum_{j=0}^{m} \binom{m}{j} = 2^m\end{aligned}$$

the $RM(m-r-1, m)$ code is the dual of the $RM(r,m)$ code. □

Exercises

3.8.8 Show that Theorem 3.8.7 holds for the codes $RM(r,m), 1 \le m \le 4$, constructed in Examples 3.8.1, 3.8.3, 3.8.4 and Exercises 3.8.5, 3.8.6.

We consider the first order Reed-Muller code $RM(1,m)$. Notice that $RM(m-2, m)$ has dimension $2^m - m - 1$ and has distance 4, length 2^m and therefore is an extended Hamming code. By Theorem 3.8.7, $RM(1,m)$ is the dual of this extended Hamming code. We present a decoding algorithm for this code which is quite efficient. We postpone a discussion of a decoding algorithm for general $RM(r,m)$ codes until Chapter 9.

Note that the $RM(1,m)$ code is a small code with a large minimum distance, so a good decoding algorithm is in fact the most elementary: for each received word w, find the codeword in $RM(1,m)$ closest to w. This can be done very efficiently.

Example 3.8.9 Let $m = 3$, consider the $RM(1,3)$ code which has length $8 = 2^3$, and $16 = 2^{3+1}$ codewords. The minimum distance is 4. Let

$$G(1,3) = \begin{bmatrix} 1111 & 1111 \\ 0101 & 0101 \\ 0011 & 0011 \\ 0000 & 1111 \end{bmatrix}$$

Note that if w is received and $d(w,c) < 2$ the we decode w to c but if $d(w,c) > 6$, then $d(w, \mathbf{1} + c) < 2$ and we decode w to $\mathbf{1} + c$. (Recall $\mathbf{1}$ is a codeword). For example, if $w =$ 1000 1111 is received then $c =$ 0000 1111 is the nearest codeword. If $w =$ (10101011) is received and we find $c =$ (01010101) with $d(w,c) > 6$, then $c + \mathbf{1} =$ 10101010 is the nearest codeword. Thus we have to examine at most half of the codewords in $RM(1,m)$

In fact, there are very efficient matrix methods to compute these distances but we will not consider them here.

Exercises

3.8.10 Let $G(1,3)$ be the generator for the $RM(1,3)$ code, decode the following received words

a. 0101 1110

b. 0110 0111

c. 0001 0100

d. 1100 1110

3.8.11 Let $G(1,4)$ be the generator for $RM(1,4)$ code, decode the following received words

a. 1011 0110 0110 1001

b. 1111 0000 0101 1111

3.9 Fast Decoding for $RM(1,m)$

In this section we present briefly and without justification a very efficient decoding method for $RM(1,m)$ codes. It utilizes the Fast Hadamard Transform to find the nearest codeword. First we need to introduce the Kronecher product of matrices.

Define $A \times B = [a_{ij}B]$; that is, entry a_{ij} in A is replaced by the matrix $a_{ij}B$.

Example 3.9.1 Let $H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ $I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ then

$$I_2 \times H = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}$$

$$H \times I_2 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}$$

Now we consider a series of matrices defined as:

$$H_m^i = I_{2^{m-i}} \times H \times I_{2^{i-1}}$$

for $i = 1, 2, \ldots, m$, where H is as in Example 3.9.1.

Example 3.9.2 Let $m = 2$. Then

$$\begin{aligned} H_2^1 &= I_2 \times H \times I_1 = I_2 \times H \\ H_2^2 &= I_1 \times H \times I_2 = H \times I_2 \end{aligned}$$

(see Example 3.9.1).

Example 3.9.3 Let $m = 3$ then

$$H_3^1 = I_4 \times H \times I_1 = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \end{bmatrix}$$

$$H_3^2 = I_2 \times H \times I_2 = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 \end{bmatrix}$$

$$H_3^3 = H \times I_4 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \end{bmatrix}$$

The recursive nature of the construction of $RM(1, m)$ codes suggests that there is a recursive approach to decoding as well. This is the intuitive basis for the following decoding algorithm for $RM(1, m)$.

Algorithm 3.9.4 Suppose w is received and $G(1, m)$ is the generator matrix for $RM(1, m)$ code

(1) replace 0 by -1 in w forming $\overline{w}$

(2) compute $w_1 = \overline{w} H_m^1$ and $w_i = w_{i-1} H_m^i$ for $i = 2, 3, \ldots, m$.

(3) Find the position j of the largest component (in absolute value) of w_m.

Let $v(j) \in K^m$ be the binary representation of j (low order digits first). Then if the j^{th} component of w_m is positive, the presumed message is $(1, v(j))$, and if it is negative the presumed message is $(0, v(j))$.

Example 3.9.5 Let $m = 3$, and $G(1, 3)$ be the generator matrix for $RM(1, 3)$ (see Example 3.8.9). If $w = 10101011$ is received convert w to $\overline{w} = (1, -1, 1, -1, 1, -1, 1, 1)$. Compute:

$$\begin{aligned} w_1 &= \overline{w} H_3^1 = (0, 2, 0, 2, 0, 2, 2, 0) \\ w_2 &= w_1 H_3^2 = (0, 4, 0, 0, 2, 2, -2, 2) \\ w_3 &= w_2 H_3^3 = (2, 6, -2, 2, -2, 2, 2, -2) \end{aligned}$$

(see Example 3.9.2 for H_3^1, H_3^2, H_3^3).

The largest component of w_3 is 6 occurring in position 1. Since $v(1) = 100$ and $6 > 0$, then the presumed message is $m = (1100)$.

Suppose $w = (10001111)$. Then $\overline{w} = (1, -1, -1, -1, 1, 1, 1, 1)$ and

$$\begin{aligned} w_1 &= \overline{w} H_3^1 = (0, 2, -2, 0, 2, 0, 2, 0) \\ w_2 &= w_1 H_3^2 = (-2, 2, 2, 2, 4, 0, 0, 0) \\ w_3 &= w_2 H_3^2 = (2, 2, 2, 2, -6, 2, 2, 2) \end{aligned}$$

the largest component of w is -6 occurring in position 4. Since $v(4) = 001$ and $-6 < 0$ the presumed message is (0001).