Why can't we have a perfect code of even distance?

If $|C| = \frac{2^n}{\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{t}}$, then all 2^n binary words of length n are partitioned into groups of size $\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{t}$.

In a code with even distance, there is at least one binary word of length n that is equidistant from 2 codewords.

3.2 Perfect codes

In the previous section we saw several bounds on the possible number of words in codes. Here we describe an important class of codes in which one of these bounds is attained.

Definition 3.9 A code C of length n and odd distance $\delta = 2t+1$ is called a *perfect code* if C attains the Hamming bound given in Theorem 3.2. That is, C is perfect iff

$$|C| = \frac{2^n}{\binom{n}{0}+\binom{n}{1}+\ldots+\binom{n}{t}}.$$

There are not very many perfect codes, but ones that do exist are very useful. The main problem in finding perfect linear codes is that $|C|$ is a power of 2, so the expression

$$\binom{n}{0}+\binom{n}{1}+\ldots+\binom{n}{t}$$

must also be a power of 2.

Example 3.10 Let $t = 0$. Then $\binom{n}{0} = 1 = 2^0$, so $|C| = \frac{2^n}{\binom{n}{0}} = 2^n$. The only code with 2^n codewords and length n is K^n, so K^n is a perfect code. (Of course, this code provides no error detection or correction.)

Example 3.11 Similarly, we can show that there is a perfect code of length $2t+1$ and distance $2t+1$ with 2 codewords: one codeword is the zero word, and the other is the word containing all 1s.

The codes from the two previous examples are not particularly interesting, and are called the *trivial* perfect codes.

In Exercise 3.4 we showed that there exists a perfect linear code with $n = 7$ and $\delta = 3$. It has 16 codewords. (Note that this code is the code discussed at the end of Subsection 2.9.)

Exercise 3.12 The *Golay* code is a perfect code with $n = 23$ and $\delta = 7$. Show that such a code may exist, and find the number of codewords in it.

$k = 12$

$2^{n-k} = 2^{23-12} = 2^{11} = 2048$

G.V. $\binom{22}{0}+\binom{22}{1}+\cdots+\binom{22}{22} = 23$

$\binom{22}{0}+\binom{22}{1}+\binom{22}{2}+\binom{22}{3}+\binom{22}{4}+\binom{22}{5} = 35443$

G.V does not show this exists

Hamming Bound: $|C| = \frac{2^{23}}{\binom{23}{0}+\binom{23}{1}+\binom{23}{2}+\binom{23}{3}} = \frac{2^{23}}{2^{11}} = 2^{12}$

2^{12} codewords.

The possible lengths and distances for a perfect code were determined by Tietavairen and van Lint in 1963. They showed that:

Theorem 3.13 *If C is a non-trivial perfect code of length n and distance $\delta = 2t+1$ then either $n = 23$ and $\delta = 7$, or $n = 2^r - 1$ for some $r \geq 2$ and $\delta = 3$.*

Note that Theorem 3.13 does not state that every code meeting those requirements will be perfect, just that every perfect code must satisfy those requirements.

Suppose C is a linear code of length n and distance $\delta = 2t + 1$. By Theorem 1.47 C will correct all error patterns of weight less than or equal to t. Thus every word of length n and weight less than or equal to t is a coset leader. There are exactly

$$\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{t}$$

such words, which is precisely the number of cosets if the code is perfect. Hence we have the following.

Theorem 3.14 *If C is a perfect code of length n and distance $\delta = 2t+1$ then C will correct all error patterns of weight less than or equal to t, and no other error patterns.*

Definition 3.15 A perfect code which corrects all error patterns of weight less than or equal to t is called a *perfect t-error correcting code.* From Theorem 3.13, the only possible values for t are $t = 1$ and $t = 3$.

3.3 Extended codes

Sometimes, increasing the length of a code by one digit or a few digits gives a new code with improved error detection or correction, which justifies the lower information rate.

Definition 3.16 Let C be a linear code of length n. The code C^* of length $n + 1$, formed from C by adding one extra digit to each $v \in C$ in order to make each $v^* \in C^*$ have even weight is called an *extended code of C.*

Note that since C is a linear code, C^* is also a linear code.

Example 3.17 At the start of our discussions on coding theory, we formed extended codes of K^2 and K^3 by adding a single parity check digit to the end of each codeword so that each codeword had even weight.

Theorem 3.18 Suppose that we form an extended code C^* by adding a digit to the end of each codeword of a linear code C. If the original code C has a $k \times n$ generating matrix $\mathbf{G}$ then the extended code C^* has a $k \times (n+1)$ generating matrix

$$\mathbf{G}^* = \begin{pmatrix} \mathbf{G} & b \end{pmatrix},$$

where the last column b of $\mathbf{G}^*$ is appended so that each row of $\mathbf{G}^*$ has even weight.

A parity check matrix for C^* can be constructed from $\mathbf{G}^*$ using Algorithm 2.13. However, the following theorem provides a quicker method to find a parity check matrix for C^*.

Theorem 3.19 If $\mathbf{H}$ is a parity check matrix for C, then a parity check matrix for C^* is given by

$$\mathbf{H}^* = \begin{pmatrix} \mathbf{H} & j \\ \mathbf{0} & 1 \end{pmatrix},$$

where j is a column containing all 1s.

Proof: We have that $\mathbf{H}$ is an $n \times (n-k)$ matrix with rank $(n-k)$. Hence $\mathbf{H}^*$ is an $(n+1) \times (n+1-k)$ matrix with rank $(n-k+1)$. Moreover,

$$\mathbf{G}^*\mathbf{H}^* = \begin{pmatrix} \mathbf{G} & b \end{pmatrix} \begin{pmatrix} \mathbf{H} & j \\ \mathbf{0} & 1 \end{pmatrix} = \begin{pmatrix} \mathbf{GH} & \mathbf{G}j + b \end{pmatrix}.$$

Now $\mathbf{GH} = \mathbf{0}$ and $\mathbf{G}j$ sums the ones in each row of $\mathbf{G}$, so from the definition of b it follows that $\mathbf{G}j + b = \mathbf{0}$. □

Exercise 3.20 Let C be the linear code with generating matrix $\mathbf{G}$ and parity check matrix $\mathbf{H}$, where

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix} \quad \text{and} \quad \mathbf{H} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Find $\mathbf{G}^*$ and $\mathbf{H}^*$ for the extended code C^*.

$$G^* = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \qquad H^* = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

If C is an (n, k, δ) linear code, what can be said about the length, dimension, distance and rate of the extended code C^*?

The length and dimension of C^* are $(n+1)$ and k, respectively. Thus, the rate of C^* is $k/(n+1)$. Notice that C^* is a slightly less efficient code than C since

$$\frac{k}{n} > \frac{k}{n+1}.$$

Let $v \in C$ be a nonzero codeword of minimum weight in C. Thus $\delta = \text{wt}(v)$. If $v^* \in C^*$ is the codeword corresponding to $v \in C$, then $\text{wt}(v^*) = \text{wt}(v)$ if $\text{wt}(v)$ is even, and $\text{wt}(v^*) = \text{wt}(v) + 1$ if $\text{wt}(v)$ is odd. Hence if C has odd distance δ, then the distance of C^* is $\delta + 1$, whereas if δ is even, then the distance of C^* is still δ. Thus an extended code is only useful when the distance of the original code is odd, in which case the extended code corrects no more errors than the original code, but it detects one more error.

When forming an extended code, there is no particular reason to add the extra digit to the end of each original codeword. A code with similar properties can be constructed by inserting an extra digit in any particular position in each codeword (as long as it is the same position in each codeword).

Exercise 3.21 Let C be the linear code $C = \{000000, 111000, 000111, 111111\}$. Form an extended code C^* by adding a parity check digit to the *start* of each codeword of C. A generating matrix and parity check matrix for C are:

$$\mathbf{G}_C = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix} \qquad \mathbf{H}_C = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Describe a generating matrix and parity check matrix for C^* in terms of $\mathbf{G}_C$ and $\mathbf{H}_C$. What are the length, dimension, distance and information rate for each of the two codes?

$G_{C^*} = (1 \quad G_C)$ $\qquad H_{C^*} = \begin{pmatrix} 1 & 0 \\ j & H \end{pmatrix}$

or

$H_{C^*} = \begin{pmatrix} 0 & 1 \\ H & j \end{pmatrix}$

Why don't we make an extended code with words of odd weight? Let $u, v \in C^*$ so $wt(u)$ odd, $wt(v)$ odd.

$wt(u+v) = wt(u) + wt(v) - 2(\#\text{of positions both have a one})$

$\neq$ odd odd even.

even.

3.4 The $(a \mid a+b)$ construction

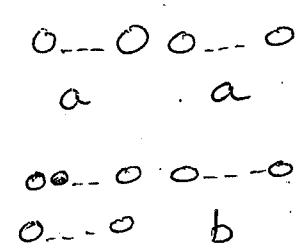
Given two codes of length n, we can combine these to form a new code of length $2n$ with good error correcting properties.

Example 3.22 Consider the following two codes of length $n = 4$:

Code A $\{0000, 0011, 0101, 0110, 1001, 1010, 1100, 1111\}$
Code B $\{0000, 1111\}$.

Define a new code C with words of length 8. The first four bits of each new codeword are a codeword a of A, and the last four bits of each codeword are obtained by adding to a a codeword b of B. Thus for each $a \in A$, there will be two new codewords in C (as there are two codewords in B), each of the form $a \mid a+b$. The new code C is:

$a \mid a+0000$	$a \mid a+1111$
00000000	00001111
00110011	00111100
01010101	01011010
01100110	01101001
10011001	10010110
10101010	10100101
11001100	11000011
11111111	11110000



Theorem 3.23 *Let A be an (n, k_A, δ_A) linear code, B be an (n, k_B, δ_B) linear code and let δ be the smaller of $2\delta_A$ and δ_B. Then the code C whose codewords are all the binary words of the form $(a \mid a+b)$, where $a \in A$ and $b \in B$, is a $(2n, k_A + k_B, \delta)$ linear code.*

Proof: The length of code C is clearly $2n$. Code A contains 2^{k_A} codewords and code B contains 2^{k_B} codewords, so the code C contains $2^{k_A} \times 2^{k_B} = 2^{k_A+k_B}$ codewords.

To verify that C has minimum distance $\delta = \min\{2\delta_A, \delta_B\}$, note firstly that C contains all codewords of the form $(a \mid a+0)$ for $a \in A$ and all codewords of the form $(0 \mid 0+b)$ for $b \in B$. Hence, $\delta \leq \min\{2\delta_A, \delta_B\}$. However, if C contains a nonzero codeword $c = (a \mid a+b)$, then either $b = 0$ and so $\mathrm{wt}(c) \geq 2\delta_A$, or $b \neq 0$ in which case

$$\mathrm{wt}(c) = \mathrm{wt}(a \mid a+b) = \mathrm{wt}(a) + \mathrm{wt}(a+b) = d(0,a) + d(a,b) \geq d(0,b)$$

by the triangle inequality and so $\mathrm{wt}(c) \geq \delta_B$. Thus in either case, $\mathrm{wt}(c) \geq \min\{2\delta_A, \delta_B\}$. □

order matters!

Example 3.24 In Example 3.22, the original codes A and B had $n = 4$, $k_A = 3$, $\delta_A = 2$, $k_B = 1$ and $\delta_B = 4$. The resulting code C is an $(8, 4, 4)$ code. If the two codes A and B are interchanged in the construction, the resulting code is only an $(8, 4, 2)$ code.

Theorem 3.25 *If A is an (n, k_A) code with generating matrix $\mathbf{G}_A$ and parity check matrix $\mathbf{H}_A$, and B is an (n, k_B) code with generating matrix $\mathbf{G}_B$ and parity check matrix $\mathbf{H}_B$, then a generatng matrix $\mathbf{G}_C$ and parity check matrix $\mathbf{H}_C$ for the code C formed by the $(a \mid a+b)$ construction are*

$$\mathbf{G}_C = \begin{pmatrix} \mathbf{G}_A & \mathbf{G}_A \\ 0 & \mathbf{G}_B \end{pmatrix}, \qquad \mathbf{H}_C = \begin{pmatrix} \mathbf{H}_A & \mathbf{H}_B \\ 0 & \mathbf{H}_B \end{pmatrix}.$$

Proof: Clearly, $\mathbf{G}_C$ is a $(k_A + k_B) \times 2n$ matrix with rank $k_A + k_B$ which generates C. $\mathbf{H}_C$ is a $2n \times (2n - k_A - k_B)$ matrix with linearly independent columns, and we have

$$\mathbf{G}_C\mathbf{H}_C = \begin{pmatrix} \mathbf{G}_A\mathbf{H}_A + 0 & \mathbf{G}_A\mathbf{H}_B + \mathbf{G}_A\mathbf{H}_B \\ 0 + 0 & 0 + \mathbf{G}_B\mathbf{H}_B \end{pmatrix} = \mathbf{0}.$$

□

3.5 Hamming codes

Definition 3.26 A linear code of length $n = 2^r - 1$, $r \geq 2$, having a parity check matrix $\mathbf{H}$ whose rows consist of all nonzero vectors of length r is called a *Hamming code* of length $2^r - 1$.

Example 3.27 One possibility for a parity check matrix $\mathbf{H}$ for a Hamming code of length 7 (so $r = 3$) is:

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

rows are all 7 non-zero vectors of length 3.

By Algorithm 2.13, a generating matrix $\mathbf{G}$ for a Hamming code of length 7 is therefore

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

code discussed at end of sec 2.9

Thus the code has dimension 4 and contains $2^4 = 16$ codewords. The distance of the code is $\delta = 3$. The information rate is $4/7$.

H contains I_r

An $n \times r$ matrix $\mathbf{H}$ whose rows are all the non-zero binary words of length r must contain each word of weight one as a row and hence must have r linearly independent columns. Hence $\mathbf{H}$ is a parity check matrix for some linear code and by definition this code is a Hamming code. Furthermore, there are precisely $2^r - 1$ non-zero binary words of length r, so $n = 2^r - 1$. Thus a Hamming code has length $n = 2^r - 1$ and has dimension $n - r = 2^r - 1 - r$, so it contains 2^{2^r-1-r} codewords.

We can find the distance of any Hamming code. No row of $\mathbf{H}$ is the zero word, so no single row of $\mathbf{H}$ is linearly dependent. No two rows of $\mathbf{H}$ are equal, so no two rows of $\mathbf{H}$ are linearly dependent. Thus C has distance at least 3. But we can clearly choose three rows of $\mathbf{H}$ (say $100\ldots0$, $0100\ldots0$, $1100\ldots0$) which form a linearly dependent set. Thus by Theorem 2.42, a Hamming code has distance $\delta = 3$.

We can investigate the Hamming bound for any Hamming code. For $n = 2^r - 1$ and $\delta = 3 = 2t + 1$ (so $t = 1$), we have

$$\frac{2^n}{\binom{n}{0} + \ldots \binom{n}{t}} = \frac{2^n}{\binom{n}{0} + \binom{n}{1}} = \frac{2^{2^r-1}}{1+n} = \frac{2^{2^r-1}}{1+2^r-1} = 2^{2^r-1-r}.$$

needs the Hamming bound.

Putting together the previous few observations, Theorem 3.14 tells us that *Hamming codes are perfect, single-error correcting codes.*

It is trivial to construct an SDA for a Hamming code. All error patterns of weight 1 are corrected, so every word of length $2^r - 1$ and weight one must be a coset leader. If e is an error pattern then $e\mathbf{H}$ sums the rows of the parity check matrix $\mathbf{H}$ corresponding to positions in which errors occurred. Hence, since $\mathbf{H}$ has $2^r - 1$ rows, an SDA for a Hamming code must be given by:

coset leader	syndrome
$000\ldots0$	$000\ldots0$
$\mathbf{I}_{2^r-1}$	$\mathbf{H}$

Example 3.28 For the Hamming code in Example 3.27, assume $w = 1101001$ is the received word. The syndrome is $w\mathbf{H} = 011$, which is the fourth row of $\mathbf{H}$. Thus the coset leader is the fourth row of I_7, $u = 0001000$. We conclude that the most likely codeword is $w + u = 1100001$.

Exercise 3.29 Use the Hamming code in Example 3.27 to determine the most likely codeword corresponding to each of the received words $w_1 = 1101011$ and $w_2 = 1111111$.

$w_1H = 001$ last row of H, so most likely error pattern 0000001

$v_1 = 1101010$.

$w_2H = 000$ so most likely no error $v_2 = 1111111$.

A Hamming code of length $2^r - 1$ is a $(2^r - 1, 2^r - 1 - r, 3)$ linear code. The advantage of using a Hamming code of long length is that it has many codewords (the maximum number of codewords possible for a given length and distance 3). However, every Hamming code is only 1-error correcting, so they are not useful if there is a high probability of errors.

Since Hamming codes have distance 3 (odd), we can gain some extra error detection capability by forming the extended Hamming code. The extended Hamming code of length 2^r is a $(2^r, 2^r - 1 - r, 4)$ linear code. They are 1-error correcting and 3-error detecting codes. The $(8, 4, 4)$ extended Hamming code was constructed in Example 3.22.

generated by columns of H.

Definition 3.30 The dual of the Hamming code of length $2^r - 1$ is called the *simplex* code of length $2^r - 1$. It is a $(2^r - 1, r, 2^{r-1})$ linear code. A simplex code is an example of a constant-weight code, since each nonzero codeword in a simplex code has weight 2^{r-1}.

$k_C + k_{C^\perp} = n$

$G_{C^\perp}$ $\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$

Exercise 3.31 Describe how you could generate the codewords in the simplex code of length 7.

Generated by columns of parity-check matrix H from previous page.

They are called simplex codes because the codewords form a simplex in Hamming space.

↑ set of equidistant points

↳ mathematical space where points are binary words of length n and distance is measured by Hamming distance

3.6 Reed-Muller codes

These codes were introduced in the 1950s by I.S. Reed and D.E. Muller. One of these codes was used by the Mariner 9 space probe to send pictures of Mars back to earth. Rather than maintaining a fixed distance (and hence error correction capacity, as did the Hamming codes), Reed-Muller codes give an increased distance as the length of codewords increases.

Mariner 9 mission to Mars

Launch: May 30, 1971
Arrival: Nov 13, 1971
Mass: 998 kilograms
Science instruments: Wide and narrow angle cameras with digital tape recorder, infrared spectrometer and radiometer, ultraviolet spectrometer, radio occultation and celestial mechanics instruments.

Mariner 9 was launched successfully on May 30, 1971, and became the first artificial satellite of Mars when it arrived on November 13, 1971 and went into orbit, where it functioned in Martian orbit for nearly a year. Mariner 9 completed its final transmission on October 27, 1972.

Upon arrival, Mariner 9 observed that a great dust storm was obscuring the whole globe of the planet. Ground controllers sent commands to the spacecraft to wait until the storm had abated, the dust had settled, and the surface was clearly visible before compiling its global mosaic of high-quality images of the Martian surface. The storm persisted for a month, but after the dust cleared, Mariner 9 proceeded to reveal a very different planet than expected – one that boasted gigantic volcanoes and a grand canyon stretching 4,800 kilometers across its surface. More surprisingly, the relics of ancient riverbeds were carved in the landscape of this seemingly dry and dusty planet. Mariner 9 exceeded all primary photographic requirements by photo-mapping 100 percent of the planet's surface. The spacecraft also provided the first closeup pictures of the two small, irregular Martian moons: Phobos and Deimos.

Mariner 9 had a radio transmitter with a power of only 20 watts, and was transmitting over a distance of 84 million miles. Despite this, near-perfect pictures were obtained. Each picture transmitted by Mariner 9 is made up of over half a million tiny picture elements forming a rectangular array. Each picture element is a uniform shade of grey, the precise shade being specified by a 9-bit binary number. Thus each picture was represented using 5,250,000 bits, in grey-scale. Given the large distances, low power, poor reliability of electronics in the transmitter and receiver, and the general background noise of space, many errors occurred in transmission. Hence it was necessary to perform extensive error correction.

Each message was divided into packets of 6 bits, and then each string of 6 bits was encoded into a 32 bit word. Thus a picture represented by 5 and a quarter million bits was transmitted using over 5 times that number of bits. The encoding was done using the first-order Reed-Muller code of length 2^5, $RM(1,5)$. This is a $(32,6,16)$ code, with 64 codewords, which can detect 15 errors and correct up to 7 errors. The rate of the $RM(1,5)$ code is only $6/32$. For each bit of information, it was necessary to transmit more than 4 bits of redundant information. However, since errors were very likely, and retransmission was not possible, this redundancy was necessary and the mission was a success.

Reed-Muller codes are linear codes of length 2^m, for some integer $m \geq 0$. The dimension of the code (and hence the number of codewords) depends on the order r of the Reed-Muller code. The rth order Reed-Muller code of length 2^m will be denoted $RM(r,m)$, where $0 \leq r \leq m$. We give a recursive definition of these codes.

1 picture = 5 250 000 bits

in groups of 6 $x_1\ x_2\ x_3\ x_4\ x_5\ x_6$ 50 message

875000 messages

$\downarrow$ $RM(1,5)$

$c_1\ c_2 \cdots \cdots c_{32}$ codewords

correct up to 7 errors

$\downarrow$

28 millions bits.

Definition 3.32 Define the rth order Reed-Muller code of length 2^m, denoted $RM(r,m)$, as follows:

1. $RM(0,m)$ is the linear code of length 2^m consisting of the zero word and the all ones word.
2. $RM(m,m)$ is the linear code of length 2^m whose codewords are all the binary words of that length, so $RM(m,m) = K^{2^m}$.
3. $RM(r,m)$ for $0 < r < m$ is obtained using the $(a \mid a+b)$ construction where $A = RM(r, m-1)$ and $B = RM(r-1, m-1)$.

Note that there are other ways to construct the Reed-Muller codes and you may have seen another construction method for first-order Reed-Muller codes in MATH2302.

Example 3.33 The Reed-Muller codes of lengths 2^0, 2^1 and 2^2 are listed below.

m	Reed-Muller codes of length 2^m
0	$RM(0,0) = \{0,1\}$
1	$RM(0,1) = \{00,11\}$ $RM(1,1) = \{00,01,10,11\}$
2	$RM(0,2) = \{0000,1111\}$ $RM(1,2) = \{(a \mid a+b) \mid a \in \{00,01,10,11\}, b \in \{00,11\}\}$ $= \{0000,0101,1010,1111,0011,0110,1001,1100\}$ $RM(2,2) = K^4$

Using Theorem 3.25, we can give a recursive definition for a generating matrix of $RM(r,m)$.

Definition 3.34 Let $\mathbf{G}_{r,m}$ be a generating matrix for $RM(r,m)$.

1. For $r = 0$ we define $\mathbf{G}_{0,m} = \begin{pmatrix} 1 & 1 & \dots & 1 \end{pmatrix}$, that is the 1×2^m matrix of ones.
2. For $r = m$, we define $\mathbf{G}_{m,m} = \begin{pmatrix} \mathbf{G}_{m-1,m} \\ 0 \dots 01 \end{pmatrix}$.
3. For $0 < r < m$, we define $\mathbf{G}_{r,m} = \begin{pmatrix} \mathbf{G}_{r,m-1} & \mathbf{G}_{r,m-1} \\ \mathbf{0} & \mathbf{G}_{r-1,m-1} \end{pmatrix}$.

Example 3.35 The generating matrices for some small Reed-Muller codes are given below.

$$\mathbf{G}_{0,0} = \begin{pmatrix} 1 \end{pmatrix} \qquad \mathbf{G}_{0,1} = \begin{pmatrix} 1 & 1 \end{pmatrix} \qquad \mathbf{G}_{1,1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$\mathbf{G}_{0,2} = \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix} \qquad \mathbf{G}_{1,2} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \qquad \mathbf{G}_{2,2} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Exercise 3.36 Determine a generating matrix for each of $RM(1,3)$ and $RM(2,3)$.

$$G_{1,3} = \begin{pmatrix} G_{1,2} & G_{1,2} \\ 0 & G_{0,2} \end{pmatrix} = \left(\begin{array}{c|c} 1111 & 1111 \\ 0101 & 0101 \\ 0011 & 0011 \\ \hline 0000 & 1111 \end{array}\right)$$

$RM(1,3)$ contains $RM(0,3)$

$$G_{2,3} = \begin{pmatrix} G_{2,2} & G_{2,2} \\ 0 & G_{1,2} \end{pmatrix} = \left(\begin{array}{c|c} 1111 & 1111 \\ 0101 & 0101 \\ 0011 & 0011 \\ 0001 & 0001 \\ \hline 0000 & 1111 \\ 0000 & 0101 \\ 0000 & 0011 \end{array}\right)$$

$RM(2,3)$ contains $RM(1,3)$

Note that $RM(1,3)$ is the $(8,4,4)$ extended Hamming code that has appeared earlier in the course.

Exercise 3.37 State the length, dimension and distance of each of the Reed-Muller codes $RM(r,m)$ for $m = 3$.

Code	$RM(0,3)$	$RM(1,3)$	$RM(2,3)$	$RM(3,3)$
Length	8	8	8	8
Dimension	1	4	7	8
Distance	8	4	2	1

Theorem 3.38 *The rth order Reed-Muller code $RM(r,m)$ defined above has the following properties:*

1. *$RM(r,m)$ has length 2^m;*
2. *$RM(r,m)$ has dimension $k = \sum_{i=0}^{r} \binom{m}{i}$;*
3. *$RM(r,m)$ has distance $\delta = 2^{m-r}$;*
4. *$RM(r-1,m)$ is contained in $RM(r,m)$, where $r > 0$;*
5. *the code $RM(m-1-r,m)$ where $r < m$ is the dual of the code $RM(r,m)$.*

The proofs of these claims are by induction and may appear in your tutorial problems or on an assignment.

The rate of $RM(r,m)$ gets very small as m gets large. However, the *distance* is very large for the length of the code, so these codes are useful in situations where errors are likely and when error detection/correction is very important.

Hadamard matrix: Square matrix whose entries are 1 and −1 and whose rows are mutually orthogonal.

Hadamard transform: take 2^m real numbers and multiply by various matrices based on Hadamard matrices to get 2^m real numbers.

3.7 Decoding of first-order Reed Muller codes

There is a fast decoding algorithm for first-order Reed-Muller codes, based on the recursive nature of these codes. The proof that this algorithm works is beyond the scope of this course. The algorithm uses some matrix trickery (Fast Hadamard Transform) to identify the nearest codeword, rather than working with syndromes and coset leaders.

Definition 3.39 The *Kronecker product* of two matrices $\mathbf{A}$ and $\mathbf{B}$ is defined by

$$\mathbf{A} \times \mathbf{B} = (a_{ij}\,\mathbf{B});$$

that is, entry a_{ij} of matrix $\mathbf{A}$ is replaced by the matrix $a_{ij}\mathbf{B}$.

$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Example 3.40 Let $\mathbf{L} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and let $\mathbf{I}_n$ be the $n \times n$ identity matrix. Then

$$\mathbf{I}_2 \times \mathbf{L} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \quad \text{and} \quad \mathbf{L} \times \mathbf{I}_2 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}.$$

Definition 3.41 We define a series of matrices based on the matrix $\mathbf{L}$ from Example 3.40. Let m be a positive integer. For $i = 1, 2, \ldots, m$, we define the matrix $\mathbf{L}_m^i$ as

$$\mathbf{L}_m^i = \mathbf{I}_{2^{m-i}} \times \mathbf{L} \times \mathbf{I}_{2^{i-1}}.$$

Example 3.42 Let $m = 2$. Then we have constructed the two matrices $\mathbf{L}_2^1$ and $\mathbf{L}_2^2$ in Example 3.40 since

$$\mathbf{L}_2^1 = \mathbf{I}_2 \times \mathbf{L} \times \mathbf{I}_1 = \mathbf{I}_2 \times \mathbf{L}$$

$$\text{and} \quad \mathbf{L}_2^2 = \mathbf{I}_1 \times \mathbf{L} \times \mathbf{I}_2 = \mathbf{L} \times \mathbf{I}_2$$

Exercise 3.43 Determine the matrix $\mathbf{L}_3^1$.

$L_3^1 = I_4 \times L \times I_1 = I_4 \times L$

$I_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

$L_3^1 = \begin{pmatrix} L & 0 & 0 & 0 \\ 0 & L & 0 & 0 \\ 0 & 0 & L & 0 \\ 0 & 0 & 0 & L \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \end{pmatrix}$

The matrices $\mathbf{L}_3^2$ and $\mathbf{L}_3^3$ are given here for your reference.

$$\mathbf{L}_3^2 = \mathbf{I}_2 \times \mathbf{L} \times \mathbf{I}_2 = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 \end{pmatrix}$$

$$\mathbf{L}_3^3 = \mathbf{I}_1 \times \mathbf{L} \times \mathbf{I}_4 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \end{pmatrix}$$

Before giving the decoding algorithm, recall that to write a natural number x in binary representation with low order digits first, you write

$$x = \alpha_0 2^0 + \alpha_1 2^1 + \alpha_2 2^2 + \cdots + \alpha_i 2^i$$

where i is the largest value such that $2^i \leq x$ and each $\alpha_j \in \{0, 1\}$, and then the binary representation of x is $\alpha_0\alpha_1\alpha_2 \ldots \alpha_i$.

The following decoding algorithm incorporates both error detection/correction and the recovery of the intended message word, so it takes a received word of length 2^m and returns a message word of length $m + 1$.

Algorithm 3.44 Decoding *$RM(1, m)$ Suppose w is the received word and $\mathbf{G}_{1,m}$ is the generating matrix for the $RM(1, m)$ code.*

1. *Replace each 0 in w by -1 to form the word $\overline{w}$.*
2. *Calculate $w_1 = \overline{w}\mathbf{L}_m^1$ and then for each $i = 2, 3, \ldots, m$ calculate $w_i = w_{i-1}\mathbf{L}_m^i$.*
3. *Determine the position j of the largest component (in absolute value) of w_m, where position is measured from left to right and counted from 0 to $2^m - 1$.*
4. *Let $v(j)$ be the binary representation of j (low order digits first).*

If the jth component of w_m is positive, then the most likely intended message word is $(1, v(j))$. If the jth component is negative, then the most likely intended message word is $(0, v(j))$.

Example 3.45 A message has been encoded using the code $RM(1, 3)$. Determine the most likely intended message word if we receive the word $w = 10101011$.

We apply Algorihtm 3.44, and write our vectors using commas for clarity.

Convert w to $\overline{w} = (1, -1, 1, -1, 1, -1, 1, 1)$. Compute

$$\begin{aligned} w_1 &= \overline{w}\mathbf{L}_3^1 = (0, 2, 0, 2, 0, 2, 2, 0) \\ w_2 &= w_1\mathbf{L}_3^2 = (0, 4, 0, 0, 2, 2, -2, 2) \\ w_3 &= w_2\mathbf{L}_3^3 = (2, 6, -2, 2, -2, 2, 2, -2) \end{aligned}$$

The largest component of w_3 is 6, occurring in position 1. Since $v(1) = 100$ and $6 > 0$, the presumed message word is 1100 (with corresponding codeword 10101010).

Exercise 3.46 A message has been encoded using the code $RM(1,3)$. Apply Algorithm 3.44 to determine the most likely transmitted codeword if we receive the word $w = 10001111$.

$\overline{w} = (1,-1,-1,-1,1,1,1,1)$

$w_1 = \overline{w} L_3^1 = (0,2,-2,0,2,0,2,0)$

$w_2 = w_1 L_3^2 = (-2,2,2,2,4,0,0,0)$

$w_3 = w_2 L_3^3 = (2,2,2,2,-6,2,2,2)$

position 4 $v(4) = 001$ and -6 is negative

so the message word is 0001.

(codeword 00001111)

3.8 The Extended Golay Code

The Voyager space mission (Voyager 1 was launched on 1 September 1977 and Voyager 2 was launched on 20 August 1977) successfully explored the planets Jupiter, Saturn, Uranus and Neptune and the two spacecraft continue their exploration as they move towards interstellar space. The Galileo spacecraft was launched on 18 October 1989, entered into orbit around Jupiter in 1995, and conducted a thorough exploration of Jupiter and its moons before making a mission-ending plunge into the planet in 2003. To send data back to Earth, each of these spacecraft used a pair of codes, one of which was the Extended Golay Code (a three error correcting code).

If we take the first-order Reed-Muller code $RM(1,3)$ and rearrange the bits in each codeword into the order $x_4x_6x_3x_2x_1x_5x_7x_8$, then we obtain the codewords of an equivalent code A with generating matrix

$$\mathbf{G}_A = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

If we then reverse the order of the first seven bits of each codeword of A, we obtain a code B which is still equivalent to $RM(1,3)$. A generating matrix for B is

$$\mathbf{G}_B = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

We can then use codes A and B to construct two new important codes (first published in 1949). The construction is similar to the $(a \mid a+b)$ construction given earlier.

codewords

$2^{k_A} * 2^{k_A} * 2^{k_B} = 2^{k_A+k_A+k_B}$

Definition 3.47 The *extended Golay code* is the code whose codewords are all of the binary words which can be written in the form

8 bits, 8 bits, 8 bits — words of length 24

$$(a_1 + b \mid a_2 + b \mid a_1 + a_2 + b),$$

dimension $k_A + k_A + k_B = 12$

where $a_1, a_2 \in A$ and $b \in B$. Equivalently, each codeword in the extended Golay code can be written as the sum of three binary words

$$(a_1 \mid 0 \mid a_1) + (0 \mid a_2 \mid a_2) + (b \mid b \mid b).$$

If $\mathbf{G}_A$ is a generating matrix for code A and $\mathbf{G}_B$ is a generating matrix for code B then a generating matrix for the extended Golay code is the 12×24 array

$$\mathbf{G} = \begin{pmatrix} \mathbf{G}_A & 0 & \mathbf{G}_A \\ 0 & \mathbf{G}_A & \mathbf{G}_A \\ \mathbf{G}_B & \mathbf{G}_B & \mathbf{G}_B \end{pmatrix}.$$

Of more use is the following version of the generating matrix, which is in standard form.

Definition 3.48 Let $\mathbf{B}$ be the 12×12 matrix:

$$\mathbf{B} = \left(\begin{array}{cccccccccccc|c} 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ \hline 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{array}\right).$$

and let $\mathbf{G}$ be the 12×24 matrix $\mathbf{G} = (\mathbf{I}_{12} \ \ \mathbf{B})$. The linear code C_{24} having $\mathbf{G}$ as generating matrix is the *extended Golay code*, which we will denote C_{24}.

Note that if $\mathbf{B}_1$ is the 11×11 matrix obtained from $\mathbf{B}$ by deleting the last row and column, then $\mathbf{B}_1$ has a cyclic left-shift structure. Note also that the positions of the ones in the first 11 places of the first row correspond to the quadratic residues mod 11 (including 0). Also, note that $\mathbf{B}^T = \mathbf{B}$.

$0^2 = 0$ $\quad 3^2 = 9$ $\quad 6^2 = 3$ $\quad 9^2 = 4$

$1^2 = 1$ $\quad 4^2 = 5$ $\quad 7^2 = 5$ $\quad 10^2 = 1$

$2^2 = 4$ $\quad 5^2 = 3$ $\quad 8^2 = 9$

$G = (I_{12}\ B)$

Theorem 3.49 **(Properties of C_{24})** We note the following important facts about C_{24}.

1. C_{24} has length 24 and dimension 12, with $|C_{24}| = 2^{12} = 4096$.
2. C_{24} has parity check matrix $\mathbf{H} = \begin{pmatrix} \mathbf{B} \\ \mathbf{I}_{12} \end{pmatrix}$.
3. Another parity check matrix for C_{24} is $\mathbf{H}' = \begin{pmatrix} \mathbf{I}_{12} \\ \mathbf{B} \end{pmatrix}$.
4. Another generating matrix for C_{24} is $\mathbf{G}' = (\ \mathbf{B}\ \ \mathbf{I}_{12}\ )$.
5. C_{24} is self-dual, so $C_{24}^{\perp} = C_{24}$. $v, w \in C_{24}$ $v \cdot w = 0$
6. The distance of C_{24} is 8.
7. C_{24} is a 3-error correcting code.
8. The weight distribution table for the codewords of C_{24} is:

wt	0	4	8	12	16	20	24
# words	1	0	759	2576	759	0	1

Proof of (2): $\mathbf{H}$ is a 24×12 matrix with linearly independent columns, and

$$\mathbf{GH} = (\ \mathbf{I}_{12}\ \ \mathbf{B}\ ) \begin{pmatrix} \mathbf{B} \\ \mathbf{I}_{12} \end{pmatrix} = \mathbf{B} + \mathbf{B} = \mathbf{0}.$$

Proof of (3): Note that $\mathbf{BB} = \mathbf{I}_{12}$. Thus $\mathbf{GH}' = (\ \mathbf{I}_{12}\ \ \mathbf{B}\ ) \begin{pmatrix} \mathbf{I}_{12} \\ \mathbf{B} \end{pmatrix} = \mathbf{I}_{12}^2 + \mathbf{B}^2 = \mathbf{I}_{12} + \mathbf{I}_{12} = \mathbf{0}$.

Proof of (4): The new generating matrix has the correct number of rows and columns, and rows are linearly independent. Also, we have $\mathbf{G}'\mathbf{H}' = \mathbf{0}$.

Proof of (5): Note that $\mathbf{I}^T = \mathbf{I}$, $\mathbf{B}^T = \mathbf{B}$ and that every row of $\mathbf{G}$ has even weight. Hence $\mathbf{GG}^T = \mathbf{0}$.

Proof of (6): There are three steps: $(1\,1\,0\ldots0)(G)$

I. *Proof that if $w \in C$, then $4 \mid \mathrm{wt}(w)$:*
Let r_i denote row i of $\mathbf{G}$. Any codeword w can be expressed as the sum of up to 12 rows of $\mathbf{G}$, so $w = r_{i_1} + \ldots + r_{i_m}$, where $m \leq 12$.
Perform induction on m:
If $m = 1$ then $\mathrm{wt}(w) = \mathrm{wt}(r_{i_1}) = 8$ or 12, as can be seen from $\mathbf{G}$.
If $m \geq 1$ then assume the hypothesis is true for m and consider $m+1$.
We know $w = (r_{i_1} + \ldots + r_{i_m}) + r_{i_{m+1}} = v + r_{i_{m+1}}$, where v is a codeword which is a sum of m rows of $\mathbf{G}$ and by our hypothesis $4 \mid \mathrm{wt}(v)$. Since the rows of $\mathbf{G}$ are mutually orthogonal, v and $r_{i_{m+1}}$ are orthogonal. Hence v and $r_{i_{m+1}}$ have $2x$ ones in common. Therefore

$$\mathrm{wt}(w) = \mathrm{wt}(v) + \mathrm{wt}(r_{i_{m+1}}) - 2(2x).$$

$4 \mid \mathrm{wt}(v)$ 57 $4 \mid \mathrm{wt}(r_{i_{m+1}})$ $4 \mid 4x$

Hence $4 \mid \mathrm{wt}(w)$.
So, by induction, statement I is true.

II. *Proof that the distance of $C_{24} = 4$ or 8:*
Since there are rows of $\mathbf{G}$ with weight 8, $d(C_{24}) \leq 8$. Clearly, the distance of $C_{24} \geq 1$, so the result follows from I.

III. *Proof that the distance of $C_{24} = 8$:*
Suppose we have a codeword w of weight 4. Then, using our two generating matrices,

$$w = u_1 (\mathbf{I}_{12} \ \mathbf{B}) = u_2 (\mathbf{B} \ \mathbf{I}_{12})$$

for some u_1 and u_2. Write $w = [w_1, w_2]$ where w_1 and w_2 have length 12. Hence one of these has weight ≤ 2. But $w_1 = u_1$ and $w_2 = u_2$. So one of u_1 or u_2 has weight ≤ 2. Thus w is the sum of either 1 or 2 rows of a generating matrix. However, the sum of any 2 rows of $\mathbf{B}$ has weight at least 6. Thus, as $\mathbf{B}$ forms part of the generating matrix concerned, $\mathrm{wt}(w) \geq 6$. Thus there are no words of weight 4, so the distance of $C_{24} = 8$. □

Proof of (7): Follows from (6).

Explanation of (8): The sum of all rows of $\mathbf{G}$ is $11\ldots1$, so $11\ldots1 \in C$. Hence the number of words of weight k equals the number of words of weight $24 - k$. Hence it is easy to verify some of the entries in the weight table for C_{24}. Clearly, there is one word of weight zero and one word of weight 24. There are no words of weight 4 (as $\delta = 8$), so there are no words of weight 20.

3.9 Decoding the Extended Golay Code

We now define an algorithm for IMLD for C_{24}. Throughout this section, we use the following notation:

- w Received word
- v Closest codeword to w
- u Error pattern ($u = v + w$)

and we assume that message words of length 12 have been encoded using the generating matrix $\mathbf{G} = (\mathbf{I}_{12} \ \mathbf{B})$.

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 C_{24} has distance 8, every error pattern of weight less than or equal to 3 must be a coset leader, so suppose we have an error pattern u where $\mathrm{wt}(u) \leq 3$. Write $u = [u_1, u_2]$ where u_1 and u_2 each have length 12.

As $\mathrm{wt}(u) \leq 3$, we must have either $\mathrm{wt}(u_1) \leq 1$ or $\mathrm{wt}(u_2) \leq 1$. Let $\mathbf{H}_1$ be the parity check matrix

$$\mathbf{H}_1 = \begin{pmatrix} \mathbf{I}_{12} \\ \mathbf{B} \end{pmatrix}.$$

u_1	u_2
3	0
2	0, 1
1	0, 1, 2
0	0, 1, 2, 3

Then we have the syndrome $s_1 = w\mathbf{H}_1 = u\mathbf{H}_1 = u_1\mathbf{I}_{12} + u_2\mathbf{B} = u_1 + u_2\mathbf{B}$.
If $\mathrm{wt}(u_2) = 0$ then $s_1 = u_1$ so $\mathrm{wt}(s_1) \leq 3$ (as $\mathrm{wt}(u_1) \leq 3$).
If $\mathrm{wt}(u_2) = 1$ then $s_1 = u_1 +$ (1 row of $\mathbf{B}$), so s_1 is a row of $\mathbf{B}$ with at most 2 digits changed (as $\mathrm{wt}(u_1) \leq 2$).

Similarly, let $\mathbf{H}_2$ be the parity check matrix

$$\mathbf{H}_2 = \begin{pmatrix} \mathbf{B} \\ \mathbf{I}_{12} \end{pmatrix}.$$

$\left(\begin{matrix} B \\ I_{12} \end{matrix}\right)$

In this case we have the syndrome $s_2 = w\mathbf{H}_2 = u\mathbf{H}_2 = u_1\mathbf{B} + u_2\mathbf{I}_{12} = u_1\mathbf{B} + u_2$.
If $\text{wt}(u_1) = 0$ then $s_2 = u_2$ so $\text{wt}(s_2) \leq 3$ (as $\text{wt}(u_2) \leq 3$).
If $\text{wt}(u_1) = 1$ then $s_2 = u_2 +$ (1 row of $\mathbf{B}$), so s_2 is a row of $\mathbf{B}$ with at most 2 digits changed (as $\text{wt}(u_2) \leq 2$).

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. There are several possibilities corresponding to the possible weights of u_1 and u_2.

- If $\text{wt}(s_1) \leq 3$ then we have $u = [u_1, 0]$. (Here $\text{wt}(u_2) = 0$.)
- If $\text{wt}(s_2) \leq 3$ then we have $u = [0, u_2]$. (Here $\text{wt}(u_1) = 0$.)
- If $\text{wt}(s_1) \geq 3$ and $\text{wt}(s_2) \geq 3$, then we look for the row of $\mathbf{B}$ which is closest to s_1 or s_2 and use this to calculate the error pattern u.

These possibilities can be used to find an algorithm for decoding. However, in the decoding process we want to use only one parity check matrix. We will use $\mathbf{H} = \mathbf{H}_1$, but noting that $\mathbf{B}^2 = \mathbf{I}_{12}$, we have

$$\begin{aligned} s_2 &= u_1\mathbf{B} + u_2 \\ &= u_1\mathbf{B} + u_2\mathbf{I}_{12} \\ &= u_1\mathbf{B} + u_2\mathbf{B}^2 \\ &= (u_1 + u_2\mathbf{B})\mathbf{B} \\ &= s_1\mathbf{B}. \end{aligned}$$

In the following algorithm, e_i is the word of length 12 with a one in the ith position and zeros elsewhere.

Algorithm 3.50 IMLD for the Extended Golay Code, C_{24}

1. Compute the syndrome $s = w\mathbf{H} = w\begin{pmatrix} \mathbf{I}_{12} \\ \mathbf{B} \end{pmatrix}$.
2. If $\text{wt}(s) \leq 3$ then $u = [s, 0]$.
3. If $\text{wt}(s + b_i) \leq 2$ for some row b_i of $\mathbf{B}$ then $u = [s + b_i, e_i]$.
4. Compute the second syndrome $s\mathbf{B}$.
5. If $\text{wt}(s\mathbf{B}) \leq 3$ then $u = [0, s\mathbf{B}]$.
6. If $\text{wt}(s\mathbf{B} + b_i) \leq 2$ for some row b_i of $\mathbf{B}$ then $u = [e_i, s\mathbf{B} + b_i]$.
7. If u is not yet determined, then more than 3 errors have occurred so request retransmission.

Of course, once u has been determined, w is decoded to $w + u$.
Algorithm 3.50 requires at most 26 weight calculations in the decoding procedure. Of course, as soon as u has been determined, no further steps in the algorithm need to be applied.

$H = \begin{pmatrix} I_{12} \\ B \end{pmatrix}$ $\quad wH = w\begin{pmatrix} I_{12} \\ B \end{pmatrix}$

Example 3.51 Decode the received word $w =$ 101 111 101 111, 010 010 010 010.
The syndrome is

sum of rows 2, 5, 8, 11 of B

$$s = wH = 101\ 111\ 101\ 111 + 001\ 111\ 101\ 110 = 100\ 000\ 000\ 001,$$

which has weight 2. Since $\mathrm{wt}(s) \leq 3$, we find that $u = [s, 0] = [100\ 000\ 000\ 001, 0]$, and conclude that $v = w + u =$ 001 111 101 110 010 010 010 010 was the codeword sent.

Because $\mathbf{G} = (\ \mathbf{I}_{12}\ \ \mathbf{B}\ )$ is in standard form and any word in K^{12} can be encoded as a message (C_{24} has dimension 12), the actual message sent occurs in the first 12 digits of the corresponding codeword v. Hence in the previous example, 001 111 101 110 was the message encoded and sent.

Example 3.52 Decode the received word $w =$ 001 001 001 101 101 000 101 000.
The syndrome is

sum of rows 1, 3, 7, 9 of B

$$s = wH = 001\ 001\ 001\ 101 + 111\ 000\ 000\ 100 = 110\ 001\ 001\ 001,$$

which has weight 5. Proceeding to Step 3 of Algorithm 3.50, we compute

$$\begin{aligned} s + b_1 &= 000\ 110\ 001\ 100 \\ s + b_2 &= 011\ 111\ 000\ 010 \\ s + b_3 &= 101\ 101\ 011\ 110 \\ s + b_4 &= 001\ 001\ 100\ 100 \\ s + b_5 &= 000\ 000\ 010\ 010 \end{aligned}$$

Then, since $\mathrm{wt}(s + b_5) \leq 2$, we have that

5th position

$$u = [s + b_5, e_5] = [000\ 000\ 010\ 010,\ 000\ 010\ 000\ 000],$$

and conclude that $v = w + u =$ 001 001 011 111 101 010 101 000 was the codeword sent.

Exercise 3.53 Decode the received word $w =$ 000 111 000 111, 011 011 010 000.

$s = w\begin{pmatrix} I_{12} \\ B \end{pmatrix} =$ 000 111 000 111 + 101 010 101 101 sum of rows 2, 3, 5, 6, 8 of B

101 101 101 010

$\mathrm{wt}(s) > 3$ so compare s with row b_i of B for $i = 1, \ldots, 12$.

All rows differ from s in more than 2 positions.

$sB =$ sum of rows 1, 3, 4, 6, 7, 9, 11 of B

$sB =$ 111 001 111 101 $\quad \mathrm{wt}(sB) > 3.$

$sB + b_4 =$ 000 001 010 000

so the most likely error pattern $u =$ 000 100 000 000, 000 001 010 000
(e_4, $sB + b_4$)

$\therefore$ The most likely codeword is $w + u$