Hadamard Codes

♠ **Hadamard Matrices and Kronecker Product**. A *Hadamard matrix* of order n is a matrix H_n with elements 1 or -1 such that $H_n H_n^t = nI_n$. For example,

$$H_1 = [1],\ H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},\ H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}.$$

An $n \times n$ Hadamard matrix with $n > 2$ exists only if 4 divides n. Since $H_n H_n^t = nI_n$, any two different rows of H_n must be orthogonal, and the matrix obtained from the permutation of rows or columns of H_n is also a Hadamard matrix, but the symmetry may be lost. Clearly $-H_n$ is also a Hadamard matrix.

These matrices were introduced by Jacques Hadamard in 1893. And yet, despite much attention by numerous mathematicians, the central question of existence has not been answered: we do not know whether or not, for every integer m, there is an orthogonal 4m by 4m matrix of plus and minus ones; this, notwithstanding that the number of such matrices seems to grow extremely rapidly with m, the combinatorial explosion coming perhaps as early as $m = 7$. Still less is known about the classification of Hadamard matrices for general m; but they have been enumerated for $m < 7$.

We denote by e_k, the k^{th} row of the $n \times n$ identity matrix I_n; the k^{th} row of H_n is denoted by h_k; finally $e = (1, 1, \ldots, 1)$ is h_1.

Theorem 1. *Let H_n be a Hadamard matrix of order $n = 4m$. For any $k = 1, 2, \ldots, n$, define the $1, -1$ vector u_k such that at most (m-1) components of the vector $v_k = h_k + u_k$ is different from the components h_k of H_n. Let $s_k = v_k H_n^t$, then the k^{th} component of s_k is at least 4m-2(m-1)= 2m+2 and the absolute value of other components are at most 2(m-1).*

Proof. Since $H_n H_n^t = nI_n$, we have $r_k = h_k H_n^t = 4n\, e_k = 4m\, e_{4m}$. Note that if w is a (-1,1) row vector of order n, then the k^{th} component of wH_n can not exceed n. We complete the proof by observing that if h_k and v_k differs in only one component, then the k^{th} component of $r_k - s_k$ is 2 and the absolute value of the other components of $r_k - s_k$ can not exceed 2. Now each time the number of nonzero components of u_k increases to j, the k^{th} component of s_k decreases by $2j$, and the absolute value of other components of s_k may increase by up to $2j$.

The *Kronecker product* also called *tensor product* or the *direct product* of two matrices A and B is defined as follows:

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \ldots & a_{1n}B \\ a_{21}B & a_{22}B & \ldots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \ldots & a_{mn}B \end{pmatrix}$$

For example

$$H_4 = H_2 \otimes H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \left[\begin{array}{cc|cc} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ \hline 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{array}\right] = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

For $n > 4$, in order to construct a Hadamard matrix of order n using the Kronecker product, n must be divisible by *8*. For example, H_{12} exists but can not be constructed from any Hadamard matrix.

A class of Hamadard matrices $H_{2n} = H_2 \otimes H_n$ was defined by Sylvester under the name of *Anallagmatic Pavement.* A *Hadamard-Sylvester* matrix viewed as pavements, cells with *1's* are colored black and those with *-1's* are colored white.

$$H_1 = \blacksquare, \quad H_2 = \begin{matrix} \blacksquare & \blacksquare \\ \blacksquare & \square \end{matrix}, \quad H_4 = \begin{matrix} \blacksquare & \blacksquare & \blacksquare & \blacksquare \\ \blacksquare & \square & \blacksquare & \square \\ \blacksquare & \blacksquare & \square & \square \\ \blacksquare & \square & \square & \blacksquare \end{matrix}, \quad H_8 = \begin{matrix} \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare \\ \blacksquare & \square & \blacksquare & \square & \blacksquare & \square & \blacksquare & \square \\ \blacksquare & \blacksquare & \square & \square & \blacksquare & \blacksquare & \square & \square \\ \blacksquare & \square & \square & \blacksquare & \blacksquare & \square & \square & \blacksquare \\ \blacksquare & \blacksquare & \blacksquare & \blacksquare & \square & \square & \square & \square \\ \blacksquare & \square & \blacksquare & \square & \square & \blacksquare & \square & \blacksquare \\ \blacksquare & \blacksquare & \square & \square & \square & \square & \blacksquare & \blacksquare \\ \blacksquare & \square & \square & \blacksquare & \square & \blacksquare & \blacksquare & \square \end{matrix}.$$

Therefore, the $n \times n$ Hadamard-Sylvester matrix H_n must have $n(n-1)/2$ white squares and $n(n+1)/2$ black square

♠ **Hadamard Codes**. Take the $4m \times 4m$ Sylvester-Hadamard matrix H_{4m} and $-H_{4m}$ and change all the -1 entries to 0's. Here is how to obtain them:

$$H_{4m} \to \widehat{H}_{4m} = [-H_{4m} + 2J_{4m}] \;\; mod\ 3 \quad \text{and} \quad -H_{4m} \to \widehat{H}'_{4m} = [H_{4m} + 2J_{4m}] \;\; mod\ 3,$$

where J_{4m} is the $4m \times 4m$ matrix whose entries are all ones. This gives us binary words of length *4m.* The binary codes formed by using *8m* rows of $\widehat{H}_{4m}$ and $\widehat{H}'_{4m}$ are called *Hadamard codes.* Here is a Hadamard code of order *16* using $H_8 = H_2 \otimes H_2 \otimes H_2$:

$$C_8 = \left\{ \begin{matrix} 1111\ 1111, 1010\ 1010, 1100\ 1100, 1001\ 1001, 1111\ 0000, 1010\ 0101, 1100\ 0011, 1001\ 0110, \\ 0000\ 0000, 0101\ 0101, 0011\ 0011, 0110\ 0110, 0000\ 1111, 0101\ 10110, 0011\ 1100, 0110\ 1001 \end{matrix} \right\};$$

a generator may be the matrix

$$G = \begin{bmatrix} 1010\ 1010 \\ 1100\ 1100 \\ 1001\ 1001 \\ 1111\ 0000 \end{bmatrix}.$$

Now by the properties of Hadamard matrices, a Hadamard code is a *[4m,2m,2m]* linear codes and it will correct any error pattern of weight *(m-1).*

Note that in order to change $\widehat{H}_{4m}$ into H_{4m} or $\widehat{H}'_{4m}$ into $-H_{4m}$we proceeded as follows:

$$H_{4m} = 2\widehat{H}_{4m} - J_{4m} \quad \text{and} \quad -H_{4m}.$$

♠ **Hadamard Codes and the Mariner 9 Mission**. To examine the process of using codes we shall look at a real application. The **Mariner 9** was a space probe whose mission was to fly by *Mars* and transmit pictures back to *Earth.* The black and white camera aboard the **Mariner 9** took the pictures, and a fine grid was then placed over the picture and for each square of the grid the degree of blackness is measured on a scale from *0* to *63.* These numbers, expressed in binary are the data that is transmitted to *Earth* (more precisely to the Jet Propulsion Laboratory of the California Institute of Technology in Pasadena). On arrival the signal is very weak and it must be amplified. Noise from space added to the signal and thermal noise from the amplifier have the effect that it happens occasionally that a signal transmitted as a *1* is interpreted by the receiver as a *0* and vice versa. If the probability that this occurs is *0.05* then by the formula

$$\Phi_p(v,w) = p^{n-d}(1-p)^d,$$

approximately 26% of all the pictures received would be incorrect. Thus, there is clearly a need to code this information with an error correcting code. Now the question is, what code should be used? Any code will increase the size of the data being sent and this creates a problem. The **Mariner 9** is a small vehicle and can not carry a huge transmitter, so the transmitted signal had to be directional, but over the long distances involved a directional signal has alignment problems. So, there was a maximum size to how much data could be transmitted at one time (while the transmitter was aligned). This turned out to be about *5* times the size of the original data, so since the data consisted of 6 bits *(0,1)* vectors of length *6*) the codewords could be about 30 bits long. The 5-repeat code was a possibility, having the advantage that it is very easy to implement, but it is only 2-error correcting. An Hadamard code based on an Hamadard-Sylvester symmetric matrix of order *32* on the other hand would be *7-error* correcting and so worth the added difficulty of implementing it. Using this code, the probability of error in the picture is reduced to only 0.01% (the *5-repeat* code would have a probability of error of about 1%).

We now turn our attention to the problems of coding and decoding the data using an Hadamard code. At first glance, coding doesn't seem to be a problem, after all there are *64* data types and *64* codewords, so any arbitrary assignment of data type to codeword will work. The problem lies in the fact that the **Mariner 9** is small, and this approach would require storing all *64 32-bit* codewords. It turns out to be more economical, in terms of space and weight, to design hardware that will actually calculate the codewords rather than read them out of a stored array. By choosing the Hadamard matrix correctly, the Hadamard code will turn out to be a linear code and so this calculation is simply multiplying the data by the generator matrix of the code. The correct choice for the Hadamard matrix is the one obtained by repeatedly taking the Kronecker product of the order *2* Hadamard matrix $H_{32} = H_2 \otimes H_2 \otimes H_2 \otimes H_2 \otimes H_2$; this is the Symmetric Hamadard-Sylvester matrix.

♣ **Hadamard Decoding Algorithm**. By using the fact that $H_{4m}H^t_{4m} = H^2_{4m} = 4m\, I_{4m}$ and Theorem 1, we use a simple scheme to decode any received word $\widehat{w}$.

Step 1. A received signal $\widehat{w}$, i.e. a sequence of *4m* zeros and ones, is first changed into its ±1 form w (by changing each *0* to *-1*)as follows: $w = 2\widehat{w} - h_1$.

Step 2. Compute $s = wH_{4m}$.

Step 3. If the received word $\widehat{w}$ is a codeword, then there are no errors and the syndrome $s = wH_{4m}$ will be either $\pm 4m\, e_k$.

Step 4. In the presence of errors, s will not be $\pm 4m\, e_k$, but if the number of errors is at most 7 then according to Theorem 1, the absolute value of the largest component may not decrease below 2m+4 and the absolute value of other components may decrease up to 2m-2. Thus the position of entry in $s = w\widehat{H}^t_{4m}$ with the largest absolute value will tell us which row of H_{4m} or $-H_{4m}$ (if it is negative) was transmitted.

Step 5. Too many errors, Impossible to decode $\widehat{w}$.

Remark. While this is the actual algorithm used to decode the **Mariner 9** signals, it is a bit slow from the computational point of view (requiring *322 multiplications and the corresponding additions* for each codeword), so a number of computational tricks are employed to reduce the actual computation to less than *1/3* of what the algorithm calls for.

Examples. Consider the Hadamard code $C_{4m} = C_8$, then

$$H_8 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}$$

corrects any single error pattern.

a. Suppose $\widehat{w} = 1100\ 0011$ is the received word, then
Step 1. $w = 2\widehat{w} - h_1 = (1, 1, -1, -1,\ -1, -1, 1, 1)$.
Step 2. $s = wH_8 = (0, 0, 0, 0, 0, 0, 8, 0)$.
Step 3. The seventh component of $s = 8e_7$ is the largest component, thus
$v = h_7 = (1, 1, -1, -1,\ -1, -1, 1, 1)$ and $\widehat{v} \equiv 2h_1 - v\ mod\ 3 = 1100\ 0011$.

b. Suppose $\widehat{w} = 1011\ 1010$ is the received word, then
Step 1. $w = 2\widehat{w} - h_1 = (1, 1, -1, 1,\ -1, 1, -1, -1)$.
Step 2. $s = wH_8 = (2, 6, -2, 2, 2, -2, -2, 2)$.
Step 4. The second component of $6 \geq 4m - 2 = 6$ is the largest component, thus
$v = h_2 = (1, -1, 1, -1, 1, -1, 1, -1)$ and $\widehat{v} \equiv 2h_1 - v\ mod\ 3 = 1010\ 1010$.

c. Suppose $\widehat{w} = 0001\ 1010$ is the received word, then
Step 1. $w = 2\widehat{w} - h_1 = (-1, -1, -1, 1,\ 1, 1, 1, 1)$.
Step 2. $s = wH_8 = (2, 2, -2, -2, -6, 2, -2, -2)$.
Step 4. The fifth component of s is -6 is the largest component in absolute value and $|-6| = 6 \geq 8 - 2 = 6$, thus
$v = -h_5 = (-1, -1, -1, -1, 1, 1, 1, 1)$ and $\widehat{v} \equiv 2h_1 - v\ mod\ 3 = 0000\ 1111$.

d. Suppose $\widehat{w} = 1111\ 1100$ is the received word, then
Step 1. $w = 2\widehat{w} - h_1 = (1, 1, 1, 1,\ 1, 1, -1, -1)$.
Step 2. $s = wH_8 = (4, 0, 0, 4, 4, 0, 0, -4)$.
Step 5. Since $4 < 4m - 2 = 6$, there are too many errors in order for us to decode.

♡ **Matlab**. We only explain the algorithm for Example b.

```
% Choose n, then define the matrix H_n.
≫ n = 8 ; H = hadamard ( n )
% Suppose the vector ŵ = 1011 1010 is received. Then w = 2ŵ−h_1 = (1,1,−1,1, −1,1,−1,−1).
≫ w0 = [ 1 0 1 1 , 1 0 1 0 ] ; w = 2 ∗ w0 − H( 1 , : )
w =                    1  1 −1  1 −1  1 −1 −1
% Find the syndrome s.
≫ s = w ∗ H
s =                    2  6 −2  2  2 −2 −2  2
% The second component of s = 6 ≥ 8 − 2 = 6 is maximal, thus the codeword is :
≫ v = H (2 , : ) , v0 = rem(2 ∗ H( 1 , : ) − v, 3)
v =                    1 −1  1 −1  1 −1  1 −1
v0 =                      1 0 1 0 1 0 1 0
```

Exercises. Use Hadamard-Sylvester matrix of order 8 to decode the following received words: $(a)\ \ \widehat{w} = 1010\ 1011$ $\quad (b)\ \ \widehat{w} = 0000\ 1011$ $\quad (c)\ \ \widehat{w} = 0100\ 1011$

♠ **Reed-Muller Codes**. Another important class of linear block codes rich in algebraic and geometric structure is the class of *Ree-Muller codes*, which includes the Extended Hamming code. It was discovered by Muller in 1954, and the first decoding algorithm was devised by Reed also in 1954. We present a recursive definition of these codes. The r^{th} order Ree-Muller code of length 2^m will be denoted by $RM(r,m)$, for $r = 0, 1, \ldots, m$.

(1) $RM(0,m) = \{00\ldots, 11\ldots 11\}, \; RM(m,m) = \mathbb{K}^{2^m}$.

(2) $RM(r,m) = \{(x, y+x) \, : \, x \in RM(r, m-1), \, y \in RM(r-1, m-1)\}$ for $= 1, 2\ldots, m-1$.

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. Now, we have

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

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 $r = 0$, define $G(0,m) = [11\ldots 11]$, for $r = 1, 2, \ldots, m-1$, define $G(r,m)$ by

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

and for $r = m$, define

$$G(m,m) = \begin{bmatrix} G(m-1, m) \\ 00\ldots 01 \end{bmatrix}.$$

For example, $G(0,1) = [\ 1\ 1\ ], \; G(0,2) = [\ 1\ 1\ 1\ 1\ ], \; G(0,3) = [\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ ]$,

$$G(1,1) = \begin{bmatrix} 11 \\ 01 \end{bmatrix}, \; G(1,2) = \begin{bmatrix} G(1,1) & G(1,1) \\ \theta & G(0,0) \end{bmatrix} = \begin{bmatrix} 11 & 11 \\ 01 & 01 \\ 00 & 11 \end{bmatrix},$$

$$G(2,2) = \begin{bmatrix} G(1,2) \\ 0001 \end{bmatrix} = \begin{bmatrix} 1111 \\ 0101 \\ 0011 \\ 0001 \end{bmatrix}, \; G(1,3) = \begin{bmatrix} G(1,2) & G(1,2) \\ \theta & G(0,2) \end{bmatrix} = \begin{bmatrix} 1111 & 1111 \\ 0101 & 0101 \\ 0011 & 0011 \\ 0000 & 1111 \end{bmatrix},$$

$$G(2,3) = \begin{bmatrix} G(2,2) & G(2,2) \\ \theta & G(1,2) \end{bmatrix} = \begin{bmatrix} 1111 & 1111 \\ 0101 & 0101 \\ 0011 & 0011 \\ 0001 & 0001 \\ 0000 & 1111 \\ 0000 & 0101 \\ 0000 & 0011 \end{bmatrix}, \text{and} \quad G(3,3) = \begin{bmatrix} G(2,3) \\ 00000001 \end{bmatrix} = \begin{bmatrix} 1111 & 1111 \\ 0101 & 0101 \\ 0011 & 0011 \\ 0001 & 0001 \\ 0000 & 1111 \\ 0000 & 0101 \\ 0000 & 0011 \\ 0000 & 0001 \end{bmatrix}.$$

Theorem 2. *The r^{th} order Reed-Muller code $RM(r,m)$ has the following properties:*

(i) The length $n = 2^m$, the distance $d = 2^{m-r}$, and the dimension $k = \displaystyle\sum_{i=0}^{r} \binom{m}{i}$.

(ii) If $r > 0$, then $RM(r-1,m)$ is contained in $RM(r,m)$.

(iii) For $r < m$, the dual code of $RM(r,m)$ is $RM(m-r-1,m)$.

We omit the proofs of these claims which are all based on induction. Note that $RM(1,m)$ is a small code with a large minimum distance; also notice that $RM(m-2,m)$ has length 2^m, dimension $2^m - m - 1$, and distance 4 which makes it an Extended Hamming code, and according to the above theorem, $RM(1,m)$ is its dual.

♣ **Decoding Algorithm for First order Reed-Muller Codes**. $RM(1,m)$ can be decoded using a Hadamard matrix of order 2 and the Kronecker product. Let $H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, then

$$H_m^j = I_{2^{m-j}} \otimes H \otimes I_{2^{j-1}}$$

for $j = 1, 2 \ldots, m$. For example,

$$H_2^1 = I_2 \otimes H \otimes I_1 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}, \quad H_2^2 = I_1 \otimes H \otimes I_2 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}$$

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

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

$$H_3^3 = I_1 \otimes H \otimes I_4 = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \end{bmatrix}$$

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 $RM(1,m)$.

♣ **Decoding Algorithm for RM(1,m)**. Suppose a word w which is a sequence of zeros and ones is received.

Step 1. Replace all the zeros by -1 in w to obtain w_0 as follows: $w_0 = 2w - e$.

Step 2. For $j = 2, 3, \ldots, m$, compute $w_1 = \widehat{w} H_m^j$ and $wj = w_{j-1} H_m^j$.

Step 3. Find the position j_0 of the largest component (in absolute value) of w_m. Let $v(j_0) \in \mathbb{K}^m$ be the binary representation of j_0

$$0 \to 000\ldots00, 1 \to 100\ldots00, 2 \to 010\ldots00, 3 \to 110\ldots00, \ldots\ldots\ldots, 2^m - 1 \to 111\ldots11.$$

If the j_0^{th} is positive, the presumed message is $[1, v(j_0)]$, and if it is negative, the presumed message is $[0, v(j_0)]$.

Examples. Consider the Reed-Muller code $RM(1,3)$ generated by the matrix $G(1,3)$.

a. Suppose $w = 1010\ 1011$ is the received word, then

Step 1. $\widehat{w}_0 = 2w - e = (1,-1,1,-1,\ 1,-1,1,1)$.

Step 2. Compute:

$$\begin{aligned} w_1 &= \widehat{w}H_3^1 = (0,2,0,2,0,2,2,0) \\ w_2 &= w_1H_3^2 = (0,4,0,0,2,2,-2,2) \\ w_3 &= w_1H_3^3 = (2,6,-2,2,-2,2,2,-2) \end{aligned}$$

Step 3. The second component of w_3 is 6 occurring in position 1. Since $v(1) = 100$ and $6 > 0$, then the presumed message is $m = 1100$.

b. Suppose $w = 1000\ 1111$ is the received word, then

Step 1. $\widehat{w} = 2w - e = (1,-1,-1,-1,\ 1,1,1,1)$.

Step 2. Compute:

$$\begin{aligned} w_1 &= \widehat{w}H_3^1 = (0,2,-2,0,2,0,2,0) \\ w_2 &= w_1H_3^2 = (-2,2,2,2,4,0,0,0) \\ w_3 &= w_1H_3^3 = (2,2,2,2,-6,2,2,2) \end{aligned}$$

Step 3. The fifth component of w_3 is -6 occurring in position 4. Since $v(4) = 001$ and $-6 < 0$, then the presumed message is $m = 0001$.

♡ **Matlab**. We only explain the algorithm for Example b.

% Choose m, then define the 2×2 Hadamard matrix H and the matrices $H_m^1,\ H_m^2,\ \ldots,\ H_m^m$.

```
≫  m = 3 ; H = hadamard(2) ;

≫   H31 = kron(eye(4), H) ; H32 = kron(kron(eye(2) , H), eye(2)) ; H33 = kron( H , eye(4) )
```

% Suppose the vector $\widehat{w} = 1000\ 1111$ is received. Then $w_0 = 2w - e = (1,-1,-1,-1,\ 1,1,1,1)$.

```
≫  w = [ 1 0 0 0 , 1 1 1 1 ] ; e = ones(1,2^m) ; w0 = 2 * w − e
 w0                      1  −1  −1  −1  −1  1  1  1
```

% Define $w_1 = w_0H_3^1,\ w_2 = w_1H_3^2$, and $w_3 = w_2H_3^3$

```
≫  w1 = w0 * H31 ,   w2 = w1 * H32 , w3 = w2 * H33 ;

w1 =                        0  2  −2  0  2  0  2  0
w2 =                       −2  2   2  2  4   0  0  0
w3 =                        2  2   2  2 −6  2  2  2
```

% $4 \to v(4) = 001$ and $-6 < 0$, so $v = 0001$.

```
≫  v = 0001
v =                        0 0 0 1
```

Exercises. Consider the Reed-Muller code $RM(1,3)$, then decode the following received words:

(a) $w = 0110\ 0111$ (b) $w = 0001\ 0100$ (c) $w = 1100\ 1110$.

♡ **Question**. If the following message were received from outer space, why might it be conjectured that it was sent by a race of human-like beings who have one arm twice as long as the other?

0011000000110001111111101100100110010011001011111000100100010010001001001100110

♠ **The Transmission of Photographs from Deep-Space**.

♢ **1965** : **Mariner 4** was the first spaceship to photograph another planet, taking 22 complete photographs of *Mars*. Each picture was broken down into 200×200 picture elements. Each element was assigned a binary 6-tuple representing one of 64 brightness levels from white (000000) to black (111111). Thus the total number of bits (i.e. binary digits) per picture was $240,000$. Data was transmitted at the rate of $8\frac{1}{3}$ bits per second and so it took 8 hours to transmit a single picture!

♢ **1969** – **1972** : Much improved pictures of *Mars* were obtained by **Mariner 6,7 and 9** (**Mariner 8**) was lost during launching). There were three important reasons for this improvement:

1. Each picture was broken down into 700×832 elements (cf. 200×200 of **Mariner 4** and 400×525 of US commercial television).
2. **Mariner 9** was the first to be put into orbit around *Mars*.
3. The powerful Hadamard [Reed-Muller(32,64,16)] code was used for error correction. The data transmission rate was increased from $8\frac{1}{3}$ to $16,200$ bits per second. Even so, picture bits were produced by **Mariner 9**'s cameras at more than $100,000$ per second, and so data had to be stored on magnetic tape before transmission.

♢ **1976** : **Viking 1** landed softly on *Mars* and returned high quality photographs. Surprisingly, transmission of a color picture in the form of binary data is almost as easy as transmission of a black-and-white one. It is achieved simply by taking the same black- and white photograph several times, each time through a different colored filter. The black-and-white pictures are then transmitted as already described and the color picture reconstructed back on *Earth.*

♢ **5 March 1979** : High-resolution color pictures of Jupiter and its moons were returned by **Voyager 1.**

♢ **12 November 1980** : **Voyager 1** returned the first high-resolution pictures of Saturn and its moons.

♢ **25 August 1981** : **Voyager 2** returned further excellent pictures of Saturn.

♢ **24 January 1986** : **Voyager 2** passes Uranus.

♢ **24 August 1989** : **Voyager 2** passes Neptune.

♡ **Answer**. Picture have actually been transmitted from *Earth* into outer space in this way. Two large prime numbers were used so that a much more detailed picture could be sent. It is reasonable to expect that a civilized recipient of such a message would be able to work out how to reconstruct the picture, since factorization of a number into prime factors is a property independent of language or notation.