ELEC 6131: Error Detecting and Correcting Codes
Lecture 5: Important Linear Block Codes

Important linear block codes:

Hamming codes:

Code length: $n = 2^m - 1$

# of information bits: $k = 2^m - 1 - m$

# of parity bits: $n - k = m$

$d_{min} = 3 \;\Rightarrow\; t = 1$

The parity check matrix of this code H contains all m-tuples except $00\cdots0$ as its columns. They are arranged to look like:

$$H = [I_m : Q].$$

Take $m = 3$,

$$H = \underbrace{\left[\begin{array}{ccc:cccc} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right]}_{I_3}.$$

Then,

$$G = [Q^T : I_{2^m - m - 1}].$$

Since H consists all the m-tuples as its columns, adding any two columns, we get another column, i.e.,

$$\underline{h}_i + \underline{h}_j + \underline{h}_k = 0.$$

So, the minimum distance of the code is not greater than 3. Also, since we do not have any two columns that add up to $\underline{0}$, the minimum distance of the code is not less than 3. Therefore, $d_{min} = 3$.

Hamming codes are perfect codes: if we form standard array, it will contain $2^n = 2^{2^m - 1}$ elements. Each row has $2^k = 2^{2^m - m - 1}$ elements. So, there will be $\frac{2^{2^m - 1}}{2^{2^m - m - 1}} = 2^m$ cosets. Therefore, in addition to $\underline{0}$ we need $2^m - 1$ coset leaders. If we take all single error patterns, we have exactly what we need. So, a Hamming code only corrects error patterns with one erroneous bit and corrects all of these. So, Hamming codes are perfect codes. The only other binary perfect code is $(23, 12)$ Golay code.

Weight distribution: let A_i be the number of codewords of weight i. Then, $A(z) = A_n z^n + A_{n-1} z^{n-1} + \cdots + A_1 z + A_0$ can be formed. It is called weight enumerator. For a Hamming code:

$$A(z) = \frac{1}{n+1}\left[(1+z)^n + n(1-z)(1-z^2)^{\frac{n-1}{2}}\right].$$

Example: consider $m = 3$.

$$n = 2^m - 1 = 2^3 - 1 = 7 \;\Rightarrow\; (7,4) \text{ code}$$

$$A(z) = \frac{1}{8}[(1+z)^7 + 7(1-z)(1-z^2)^3]$$

$$= 1 + 7z^3 + 7z^4 + z^7.$$

Reed-Muller codes (RM codes):

Length: $n = 2^m$

Dimension: $k(r,m) = 1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r}$, where $\binom{m}{i} = \frac{m!}{i!(m-i)!}$

Minimum distance: $d_{min} = 2^{m-r}$

Let $m = 5$ and $r = 2$, then $k(2,5) = 1 + \binom{5}{1} + \binom{5}{2} = 16$. Therefore, we get a $(32, 16)$ RM code with $d_{min} = 8$. To form the generator matrix an RM code we form:

$$\underline{v}_1 = (010101 \cdots 01) \text{ of length } 2^m = n$$

$$\text{and } \underline{v}_2 = (00110011 \cdots 0011) \text{ of length } 2^m = n$$

$$\text{and } \underline{v}_3 = (00001111 \cdots 00001111) \text{ of length } 2^m = n$$

and so on, i.e.,

$$\underline{v}_i = (\underbrace{0 \cdots 0}_{2^{i-1}}, \underbrace{1 \cdots 1}_{2^{i-1}}, 0 \cdots 0, \cdots, \underbrace{1 \cdots 1}_{2^{i-1}}).$$

Then, the generator matrix is spanned by:

$$\{\underline{v}_0, \underline{v}_1, \cdots, \underline{v}_m, \underline{v}_1 \cdot \underline{v}_2, \cdots, \underline{v}_{m-1} \cdot \underline{v}_m, \underline{v}_1 \cdot \underline{v}_2 \cdot \underline{v}_3, \cdots\},$$

i.e., product of products of $\underline{v}_i$'s up to r of them.

$$G_{RM}(r,m) = \{\underline{v}_0, \underline{v}_1, \cdots, \underline{v}_m, \underline{v}_1\underline{v}_2, \underline{v}_1\underline{v}_3, \cdots, \underline{v}_{m-1}\underline{v}_m, \cdots \text{up to products of degree } r\}.$$

$\underline{v}_0 = (11 \cdots 11)$ all 1 vector of length 2^m. There are,

$$1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r}$$

vectors in $G_{RM}(r,m)$. So, the code has dimension $k(r,m) = \sum_{i=0}^{r} \binom{m}{i}$. We can arrange the vectors in $G_{RM}(r,m)$ as rows of a generator matrix.

Note that according to above construction:

$$RM(0,m) \subset RM(1,m) \subset RM(2,m) \subset \cdots \subset RM(r,m).$$

Example: let $m = 4$ and $r = 2$. Then, $n = 2^m = 2^4 = 16$.

$$k(2,4) = 1 + \binom{4}{1} + \binom{4}{2} = 1 + 4 + 6 = 11.$$

Let:

$$\underline{v}_0 = 1111111111111111$$

$$\underline{v}_4 = 0000000011111111 \leftarrow 2^{i-1} = 2^3 = 8$$

$$\underline{v}_3 = 0000111100001111 \leftarrow 2^{i-1} = 2^2 = 4$$

$$\underline{v}_2 = 0011001100110011$$

$$\underline{v}_1 = 0101010101010101$$

$$\underline{v}_3\underline{v}_4 = 0000000000001111$$

$$\underline{v}_2\underline{v}_4 = 0000000000110011$$

$$\underline{v}_1\underline{v}_4 = 0000000001010101$$

$$\underline{v}_2\underline{v}_3 = 0000001100000011$$

$$\underline{v}_1\underline{v}_3 = 0000010100000101$$

$$\underline{v}_1\underline{v}_2 = 0001000100010001.$$

The above vectors if put together do not generate a systematic code. We can turn this matrix to a systematic one with elementary row and column operations.

Decoding of RM code can be done using majority logic decoding algorithm.

Another way to construct RM codes:

Definition: Kronecker product: let matrix A be:

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{n,n} \end{bmatrix},$$

and B another $m \times m$ matrix. The Kronecker product of $A \otimes B$ is defined as:

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1}B & a_{n2}B & \cdots & a_{nn}B \end{bmatrix}.$$

Note: matrices A and B do not have to be square matrices in order to have Kronecker product. But we are only interested in this case.

Example: Hadamard matrices:

Let H be an $n \times n$ Hadamard matrix. Then, $\begin{bmatrix} H & H \\ H & -H \end{bmatrix}$ is a Hadamard matrix of order $2n$. Let $H_1 = [1]$ and $H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ and $H_{2^k} = \begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{bmatrix} = H_2 \otimes H_{2^{k-1}}$. That is, $H_4 = H_2 \otimes H_2 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & +1 \end{bmatrix}$. H_8, H_{16}, and so on could be found the same way.

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

$$G_{(2^2,2^2)} \triangleq \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Then,

$$G_{(2^3,2^3)} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

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

If we take the rows of $G(8,8)$ with weights 2^2 and 2^3 we get

$$G_{RM(1,3)} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix},$$

which is the generator matrix of an $(8, 4)$ Reed-Muller code with $d_{min} = 4$.

Example: let $m = 4$.

$$G_{(16,16)} = G_{(2,2)} \otimes G_{(2,2)} \otimes G_{(2,2)} \otimes G_{(2,2)}$$

or

$$G_{(2^4,2^4)} = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{bmatrix}.$$

If we take the rows of $G_{(16,16)}$ with weights $2^2, 2^3, 2^4$, we get:

$$G_{\mathrm{RM}}(2, 4) = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1
\end{bmatrix},$$

which is the generator polynomial of RM(2, 4) code.

Code combination:

Let $\underline{u} = (u_0, u_1, \cdots, u_{n-1})$ and $\underline{v} = (v_0, v_1, \cdots, v_{n-1})$ both over $GF(2)$. For the $2n$-tuple:

$$|\underline{u}|\underline{u} + \underline{v}| \triangleq (u_0, u_1, \cdots, u_{n-1}, u_0 + v_0, u_1 + v_1, \cdots, u_{n-1} + v_{n-1}).$$

Now assume that we have two codes:

C_1 is an (n, k_1) code with $d_{min} = d_1$

C_2 is an (n, k_2) code with $d_{min} = d_2$.

Suppose that $d_2 > d_1$. Form the following code:

$$C = |C_1 \, |C_1 \, + C_2| = \{|\underline{u}|\underline{u} + \underline{v}|: \underline{u} \in C_1 \; and \; \underline{v} \in C_2\}.$$

C is a binary $(2n, k_1 + k_2)$ linear code with generator matrix $G = \begin{bmatrix} G_1 & G_1 \\ 0 & G_2 \end{bmatrix}$. It can be shown (see the text) that $d_{min}(C) = \min\{2d_1, d_2\}$.

Example: assume that C_1 is the $(8, 4)$ code we had in the previous example:

$$G_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

and C_2 is $(8, 1)$ repetition code:

$$G_2 = [1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1].$$

Then, $G = \begin{bmatrix} G_1 & G_1 \\ \underline{0} & G_2 \end{bmatrix}$

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix},$$

which is the generator matrix of a $(16, 5)$ code with $d_{min} = 8$.

Construction of RM(r, m) from RM$(r, m-1)$ and RM$(r-1, m-1)$: Reed-Muller codes of length 2^m can be constructed using RM codes of 2^{m-1}. For $m \geq 2$ we have:

$$\text{RM}(r, m) = \{|\underline{u}|\underline{u} + \underline{v}|: \underline{u} \in RM(r, m-1) \; and \; \underline{v} \in RM(r-1, m-1)\},$$

With generator polynomial:

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

Golay code:

$(32, 12)$ Golay code is another (and only) other perfect binary code.

$$n - k = 23 - 12 = 11$$

$$2^{11} = 2048 = 1 + \binom{23}{1} + \binom{23}{2} + \binom{23}{3} = 1 + 23 + 253 + 1771.$$

That is, Golay code can correct 23-bit patterns with 3 or less errors.

$$d_{min} = 7 \;\Rightarrow\; t = \left\lfloor \frac{7-1}{2} \right\rfloor = 3.$$

An extra parity bit can be added to create a $(24, 12)$ extended Golay code with $d_{min} = 8$. This code is no more a perfect code. It can correct 3 or fewer errors and detect up to 4 errors.

The generator matrix of Golay$(24, 12)$ code can be written as:

$$G = [P : I_{12}],$$

where I_{12} is a 12×12 identity matrix and P is a 12×12 parity matrix:

$$\mathbf{P} = \begin{bmatrix} 100011101101 \\ 000111011011 \\ 001110110101 \\ 011101101001 \\ 111011010001 \\ 110110100011 \\ 101101000111 \\ 011010001111 \\ 110100011101 \\ 101000111011 \\ 010001110111 \\ 111111111110 \end{bmatrix}.$$

Parity matrix P of Golay$(24, 12)$ code

Note that P has the following properties:

1) It is symmetrical with respect to its diagonal.
2) The ith column is the transpose of the ith row.
3) $P \cdot P^T = I \;\Rightarrow\; P^T = P$.
4) The submatrix obtained by deleting last row and last column can be formed by cyclically shifting the first row to the left 11 times or, shifting the first column upward 11 times.

The parity check matrix is

$$H = [I_{12} : P^T] = [I_{12} : P].$$

So, the Golay code is self-dual.

Decoding of $(24, 12)$ Golay code: let $u^{(i)}$ be a 12-bit pattern with 0 everywhere except a 1 in i-th place. For example:

$$u^{(0)} = (10 \cdots 0)$$

$$u^{(1)} = (01 \cdots 0)$$

$$\vdots$$

$$u^{(10)} = (000000000010)$$

$$u^{(11)} = (0 \cdots 01)$$

Multiplying $u^{(i)}$ by P we get the i-th row of P, denote it by $\underline{p_i}$.

$$\underline{p_i} = u^{(i)} \cdot P.$$

Let $\underline{e}$ be an error pattern. We can write it as $\underline{e} = (\underline{x}, \underline{y})$ where $\underline{x}$ and $\underline{y}$ are 12-bit error patterns for first 12 or second 12 bits. Let's form the syndrome:

$$\underline{s} = \underline{r} \cdot H^T = \big(\underline{v} + \underline{e}\big)H^T = \underline{e} \cdot H^T$$

$$\underline{s} = \big(\underline{x}, \underline{y}\big)\begin{bmatrix} I_{12} \\ P \end{bmatrix} = \underline{x} \cdot I_{12} + \underline{y} \cdot P = \underline{x} + \underline{y} \cdot P$$

$$\underline{s} = \underline{x} + \underline{y} \cdot P \;\Rightarrow\; \underline{s} + \underline{x} = \underline{y} \cdot P \;\Rightarrow\; \underline{y} = (\underline{s} + \underline{x}) \cdot P$$

The code can correct any error pattern with weight less than or equal 3, $w(\underline{e}) \leq 3$. We have 4 situations:

1) $w\left(\underline{y}\right) = 0$, $w(\underline{x}) \leq 3$.
2) $w\left(\underline{y}\right) = 1$, $w(\underline{x}) \leq 2$.
3) $w\left(\underline{y}\right) = 2$, $w(\underline{x}) \leq 1$.
4) $w\left(\underline{y}\right) = 3$, $w(\underline{x}) = 0$.

For each of the four possibilities we denote $\underline{e}^{(i)}$ as the error pattern. That is if $w\left(\underline{y}\right) = 0 \Rightarrow \underline{e}^{(0)}$, $w\left(\underline{y}\right) = 1 \Rightarrow \underline{e}^{(1)}, \cdots$.

1) Suppose $w\left(\underline{y}\right) = 0 \Rightarrow e^{(0)}$
$$\underline{y} = \big(\underline{s} + \underline{x}\big) \cdot P \;\Rightarrow\; \underline{0} = \underline{s} + \underline{x} \;\Rightarrow\; \underline{x} = \underline{s} \;\Rightarrow\; e^{(0)} = \big(\underline{s}, \underline{0}\big).$$
2) $\underline{e} = e^{(1)}$ and let $\underline{y} = u^{(i)}$. Then,
$$\underline{s} = \underline{x} + u^{(i)} \cdot P = \underline{x} + \underline{p_i} \;\Rightarrow\; \underline{x} = \underline{s} + \underline{p_i} \;\Rightarrow\; w(\underline{s} + \underline{p_i}) \leq 2.$$
3) $\underline{e} = e^{(2)}$ or $e^{(3)}$ and $w\big(\underline{x}\big) = 0$. Then,
$$\underline{y} = \underline{s} \cdot P$$
and $w\big(\underline{s} \cdot P\big) = w\left(\underline{y}\right) = 2 \; or \; 3$. So, $\underline{e} = (\underline{0}, \underline{s} \cdot P)$.

4) $\underline{e} = e^{(2)}$ and $w(\underline{x}) = 1$. Then,

$$\underline{x} = u^{(i)}$$

$$\underline{y} = (\underline{s} + u^{(i)}) \cdot P = \underline{s} \cdot P + u^{(i)} \cdot P = \underline{s} \cdot P + \underline{p}_i$$

$$w\left(\underline{s} \cdot P + \underline{p}_i\right) = w\left(\underline{y}\right) = 2$$

So, $\underline{e} = (u^{(i)}, \underline{s} \cdot P + \underline{p}_i)$.

Following algorithm decodes $(24, 12)$ code based on the above discussion:

- Compute the syndrome $\mathbf{s}$ of the received sequence $\mathbf{r}$.
- If $w(\mathbf{s}) \leq 3$, then set $\mathbf{e} = (\mathbf{s}, \mathbf{0})$ and go to step 8.
- If $w(\mathbf{s} + \mathbf{p}_i) \leq 2$ for some row $\mathbf{p}_i$ in $\mathbf{P}$, then set $\mathbf{e} = (\mathbf{s} + \mathbf{p}_i, \mathbf{u}^{(i)})$ and go to step 8.
- Compute $\mathbf{s} \cdot \mathbf{P}$.
- If $w(\mathbf{s} \cdot \mathbf{P}) = 2$ or 3, then set $\mathbf{e} = (\mathbf{0}, \mathbf{s} \cdot \mathbf{P})$ and go to step 8.
- If $w(\mathbf{s} \cdot \mathbf{P} + \mathbf{p}_i) = 2$ for some row $\mathbf{p}_i$ in $\mathbf{P}$, then set $\mathbf{e} = (\mathbf{u}^{(i)}, \mathbf{s} \cdot \mathbf{P} + \mathbf{p}_i)$ and go to step 8.
- If the syndrome does not correspond to a correctable error pattern, stop the decoding process, or request a retransmission. (This represents a decoding failure.)
- Set the decoded codeword $\mathbf{v}^* = \mathbf{r} + \mathbf{e}$ and stop.