Cyclic codes:

Definition: a linear block code is cyclic if a cycle shift of any codeword is another codeword.

The $i$th shift of $v = (v_0, v_1, \ldots, v_{n-1})$ is:

$$v^{(i)} = (v_{n-i}, v_{n-i+1}, \ldots, v_{n-1}, v_0, v_1, \ldots, v_{n-i-1}).$$

For example, $v^{(1)} = (v_{n-1}, v_0, v_1, \ldots, v_{n-2})$ and $v^{(2)} = (v_{n-2}, v_{n-1}, v_0, v_1, \ldots, v_{n-3})$.

Example:

A (7, 4) cyclic code generated by $g(X) = 1 + X + X^3$.

<table>
<thead>
<tr>
<th>Messages</th>
<th>Code vectors</th>
<th>Code polynomials</th>
</tr>
</thead>
<tbody>
<tr>
<td>(0000)</td>
<td>0000000</td>
<td>$0 = 0 \cdot g(X)$</td>
</tr>
<tr>
<td>(1000)</td>
<td>1101000</td>
<td>$1 + X + X^3 = 1 \cdot g(X)$</td>
</tr>
<tr>
<td>(0100)</td>
<td>0110100</td>
<td>$X + X^2 + X^4 = X \cdot g(X)$</td>
</tr>
<tr>
<td>(1100)</td>
<td>1011110</td>
<td>$1 + X^2 + X^3 + X^4 = (1 + X) \cdot g(X)$</td>
</tr>
<tr>
<td>(0010)</td>
<td>0011101</td>
<td>$X^2 + X^3 + X^5 = X^2 \cdot g(X)$</td>
</tr>
<tr>
<td>(1010)</td>
<td>1110010</td>
<td>$1 + X + X^2 + X^5 = (1 + X^2) \cdot g(X)$</td>
</tr>
<tr>
<td>(0110)</td>
<td>0101100</td>
<td>$X + X^3 + X^4 + X^5 = (X + X^2) \cdot g(X)$</td>
</tr>
<tr>
<td>(1110)</td>
<td>1000110</td>
<td>$1 + X^4 + X^5 = (1 + X + X^2) \cdot g(X)$</td>
</tr>
<tr>
<td>(0001)</td>
<td>0001101</td>
<td>$X^3 + X^4 + X^6 = X^3 \cdot g(X)$</td>
</tr>
<tr>
<td>(1001)</td>
<td>1100101</td>
<td>$1 + X + X^4 + X^6 = (1 + X^3) \cdot g(X)$</td>
</tr>
<tr>
<td>(0101)</td>
<td>0111001</td>
<td>$X + X^2 + X^3 + X^6 = (X + X^3) \cdot g(X)$</td>
</tr>
<tr>
<td>(1101)</td>
<td>1010001</td>
<td>$1 + X^2 + X^6 = (1 + X + X^3) \cdot g(X)$</td>
</tr>
<tr>
<td>(0011)</td>
<td>0010111</td>
<td>$X^2 + X^4 + X^5 + X^6 = (X^2 + X^3) \cdot g(X)$</td>
</tr>
<tr>
<td>(1011)</td>
<td>1111111</td>
<td>$1 + X + X^2 + X^3 + X^4 + X^5 + X^6 = (1 + X^2 + X^3) \cdot g(X)$</td>
</tr>
<tr>
<td>(0111)</td>
<td>0100011</td>
<td>$X + X^5 + X^6 = (X + X^2 + X^3) \cdot g(X)$</td>
</tr>
<tr>
<td>(1111)</td>
<td>1001011</td>
<td>$1 + X^3 + X^5 + X^6 = (1 + X + X^2 + X^3) \cdot g(X)$</td>
</tr>
</tbody>
</table>

Let $v(X) = v_0 + v_1X + v_2X^2 + \ldots + v_{n-1}X^{n-1}$ be the polynomial representation of $v$. Then,

$$v^{(i)}(X) = v_{n-i} + v_{n-i+1}X + \ldots + v_{n-1}X^{i-1} + v_{i}X^i + v_{i+1}X^{i+1} + \ldots + v_{n-i-1}X^{n-1}.$$

Multiply $X^i$ by $v(X)$, i.e., shift $v$ $i$ times (linearly, not cyclically). Then,

$$X^i v(X) = v_0X^i + v_1X^{i+1} + \ldots + v_{n-i}X^{n-1} + \ldots + v_{n-i+1}X^{n+i-1}.$$

Add $X^i v(X)$ and $v^{(i)}(X)$:
\[ X^i v(X) + v^{(i)}(X) = v_{n-i} + v_{n-i+1}X + \cdots + v_{n-1}X^{i-1} + v_{n-i}X^n + v_{n-i+1}X^{n+1} + \cdots + v_{n-1}X^{n+i-1} \]

or:

\[ X^i v(X) + v^{(i)}(X) = [v_{n-i} + v_{n-i+1}X + \cdots + v_{n-1}X^{i-1}](X^n + 1). \]

So:

\[ X^i v(X) = q(X)[X^n + 1] + v^{(i)}(X). \]

That is, the \( i \)th cyclic shift of \( v(X) \) is generated by dividing \( X^i v(X) \) by \( X^n + 1 \).

**Theorem 1:** the non-zero code polynomial with minimum degree in a cyclic code \( C \) is unique.

**Proof:** let \( g(X) = g_0 + g_1X + \cdots + g_{r-1}X^{r-1} + X^r \) be the minimal degree code polynomial of \( C \). Suppose there is another \( g'(X) = g'_0 + g'_1X + \cdots + g'_{r-1}X^{r-1} + X^r \). Then, \( g(X) + g'(X) \) is another codeword in \( C \) with degree less than \( r \). \( \Rightarrow \) contradiction.

**Theorem 2:** let \( g(X) = g_0 + g_1X + \cdots + g_{r-1}X^{r-1} + X^r \) be the minimum degree polynomial of a cyclic code \( C \). Then, \( g_0 \neq 0 \).

**Proof:** if \( g_0 = 0 \) then shifting \( g(X) \) once to the left (or \( n-1 \) times to right) results in \( g_1 + g_2X + \cdots + g_{r-1}X^{r-2} + X^{r-1} \) which has a degree \( < r \) \( \Rightarrow \) contradiction. So, \( g(X) = 1 + g_1X + \cdots + g_{r-1}X^{r-1} + X^r \).

Let \( g(X) \) be the polynomial of minimum degree of a code \( C \). Take \( g(X), Xg(X), X^2g(X), \ldots, X^{n-r-1}g(X) \). These are shifts of \( g(X) \) by \( 0, 1, \ldots, n-r-1 \). So, they are codewords. Any linear combination of them is also a codeword. Therefore,

\[ v(X) = u_0 g(X) + u_1 X g(X) + \cdots + u_{n-r-1} X^{n-r-1} g(X) = [u_0 + u_1 X + \cdots + u_{n-r-1} X^{n-r-1}] g(X) \]

is also a code.

**Theorem 3:** let \( g(X) = 1 + g_1X + \cdots + g_{r-1}X^{r-1} + X^r \) be the non-zero code polynomial of minimum degree of an \((n, k)\) cyclic code \( C \). A binary polynomial of degree \( n-1 \) or less is a code polynomial if and only if it is a multiple of \( g(X) \).

**Proof:** let \( v(X) \) be a polynomial of degree \( n-1 \) or less such that:

\[ v(X) = (a_0 + a_1X + \cdots + a_{n-r-1}X^{n-r-1})g(X). \]

Then,

\[ v(X) = a_0 g(X) + a_1 X g(X) + \cdots + a_{n-r-1} X^{n-r-1} g(X). \]

Since \( g(X), Xg(X), \cdots \) are each codeword of \( C \) so is their sum \( v(X) \).

Now assume \( v(X) \) be a code polynomial in \( C \). Then write:
\[ v(X) = a(X)g(X) + b(X) \]
i.e., divide \( v(X) \) by \( g(X) \) and get remainder \( b(X) \) and quotient \( a(X) \).

\[ b(X) = v(X) + a(X)g(X). \]

\( v(X) \) is a codeword and so is \( a(X)g(X) \). Therefore, \( b(X) \) is also a codeword. But degree of \( b(X) \) is less than \( r \) ⇒ contradiction unless if \( b(X) = 0 \).

The number of polynomials of degree \( n - 1 \) or less that are multiple of \( g(X) \) is \( 2^{n-r} \). Due to 1-to-1 correspondence between these polynomials and the codewords (Theorem 3), we have \( 2^{n-r} = 2^k \) ⇒ \( r = n - k \).

**Theorem 4:** in an \((n,k)\) cyclic code, there is one and only one code polynomial of degree \( n - k \),

\[ g(X) = 1 + g_1X + g_2X^2 + \cdots + g_{n-k-1}X^{n-k-1} + X^{n-k}. \]

Every code polynomial is a multiple of \( g(X) \). Every binary polynomial of degree \( n - 1 \) or less that is a multiple of \( g(X) \) is a code polynomial. So,

\[ v(X) = u(X)g(X) \]

is a code polynomial, however, not in a systematic form.

To make code systematic, multiply the information polynomial \( u(X) \) by \( X^{n-k} \). This means placing the \( k \) information bits at the head of the shift register (in \( k \) right-most Flip-Flops). Then,

\[ u(X) = u_0 + u_1X + \cdots + u_{k-1}X^{k-1} \]

will result in:

\[ X^{n-k}u(X) = u_0X^{n-k} + u_1X^{n-k+1} + \cdots + u_{k-1}X^{n-1}. \]

Now divide \( X^{n-k}u(X) \) by \( g(X) \) to get:

\[ X^{n-k}u(X) = a(X)g(X) + b(X), \]

where \( b(X) \) is a polynomial of degree \( n - k - 1 \) or less:

\[ b(X) = b_0 + b_1X + \cdots + b_{n-k-1}X^{n-k-1} \]

\[ b(X) + X^{n-k}u(X) = a(X)g(X). \]

This means that \( b(X) + X^{n-k}u(X) \) is the representation of a codeword in systematic form, i.e.,

\[ b(X) + X^{n-k}u(X) = b_0 + b_1X + \cdots + b_{n-k-1}X^{n-k-1} \]

\[ + u_0X^{n-k} + u_1X^{n-k+1} + \cdots + u_{k-1}X^{n-1} \]

that represents

\[ v = (b_0, b_1, \cdots, b_{n-k-1}, u_0, u_1, \cdots, u_{k-1}). \]
**Example:** consider the $(7,4)$ cyclic code generated by $g(X) = 1 + X + X^3$. Let $u(X) = 1 + X^3$. Then,

1. $X^3 u(X) = X^3 + X^6$

2. 

![Diagram](image)

3. $v(X) = b(X) + X^3 u(X) = X + X^2 + X^3 + X^6$ or $v = (0, 1, 1, 1, 0, 0, 1)$

<table>
<thead>
<tr>
<th>Message</th>
<th>Codeword</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000</td>
<td>00000000</td>
</tr>
<tr>
<td>1000</td>
<td>11010000</td>
</tr>
<tr>
<td>0100</td>
<td>01101000</td>
</tr>
<tr>
<td>1100</td>
<td>10111000</td>
</tr>
<tr>
<td>0010</td>
<td>11100100</td>
</tr>
<tr>
<td>1010</td>
<td>00110100</td>
</tr>
<tr>
<td>0110</td>
<td>10001100</td>
</tr>
<tr>
<td>1110</td>
<td>01011110</td>
</tr>
<tr>
<td>0001</td>
<td>10100011</td>
</tr>
<tr>
<td>1001</td>
<td>01110001</td>
</tr>
<tr>
<td>0101</td>
<td>11001011</td>
</tr>
<tr>
<td>1101</td>
<td>00011111</td>
</tr>
<tr>
<td>0011</td>
<td>01000111</td>
</tr>
<tr>
<td>1011</td>
<td>10011011</td>
</tr>
<tr>
<td>0111</td>
<td>00110111</td>
</tr>
<tr>
<td>1111</td>
<td>11111111</td>
</tr>
</tbody>
</table>

A $(7,4)$ cyclic code in systematic form generated by $g(X) = 1 + X + X^3$.

**Theorem 5:** the generator polynomial of an $(n,k)$ code is a factor of $X^n + 1$.

**Proof:** divide $X^k g(X)$ by $X^n + 1$.

$$X^k g(X) = (X^n + 1) + g^{(k)}(X) \text{ or } X^n + 1 = X^k g(X) + g^{(k)}(X)$$

$g^{(k)}(X)$ is a code polynomial. So, $g^{(k)}(X) = a(X)b(X)$ for some $a(X)$. So,

$$X^n + 1 = [X^k + a(X)]g(X). \quad QED$$
**Theorem 6**: if $g(X)$ is a polynomial of degree $n - k$ and is a factor of $X^n + 1$. Then $g(X)$ generates an $(n, k)$ cyclic code.

**Proof**: let $g(X), Xg(X), \cdots, X^{k-1}g(X)$. They are all polynomials of degree $n - 1$ or less. A linear combination of them:

\[
v(X) = u_0g(X) + u_1Xg(X) + \cdots + u_{k-1}X^{k-1}g(X)
\]

\[
= [u_0 + u_1X + \cdots + u_{k-1}X^{k-1}]g(X)
\]

is a code polynomial since $u_i \in \{0, 1\}$. Then $v(X)$ will have $2^k$ possibilities. These $2^k$ polynomials form the $2^k$ codewords of the $(n, k)$ code.

**Generator polynomial of a cyclic code:**

\[
G = \begin{bmatrix}
g_0 & g_1 & g_2 & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\
0 & g_0 & g_1 & g_2 & \cdots & g_{n-k} & 0 & \cdots & 0 \\
0 & 0 & g_0 & g_1 & g_2 & \cdots & \cdots & g_{n-k} & 0 & \cdots \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & 0 & g_0 & g_1 & g_2 & \cdots & g_{n-k} & \\
\end{bmatrix}
\]

For example, for $(7, 4)$ code with $g(X) = 1 + X + X^3, g_0 = g_1 = g_3 = 1$ and $g_i = 0$ otherwise.

\[
G = \begin{bmatrix}
1 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 1 \\
\end{bmatrix}
\]

This is not always in systematic form. We can make it into systematic form by row and column operations. For example, for the $(7, 4)$ code:

\[
G' = \begin{bmatrix}
g_0 \\
g_1 \\
g_0 + g_2 \\
g_0 + g_1 + g_2 \\
\end{bmatrix} = \begin{bmatrix}
1 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 1 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 1 \\
\end{bmatrix}
\]

**Parity check matrix of cyclic codes:**

We saw that $g(X)$ divides $X^n + 1$. Write

\[
X^n + 1 = g(X)h(X),
\]

where $h(X)$ is a polynomial of degree $k$

\[
h(X) = h_0 + h_1X + \cdots + h_kX^k.
\]

Consider a code polynomial $v(X)$
\[ v(X)h(X) = u(X)g(X)h(X) \]
\[ = u(X)(X^n + 1) \]
\[ = u(X)X^n + u(X). \]

Since \( u(X) \) has degree less than or equal to \( k - 1 \), so \( u(X)X^n + u(X) \) does not have \( X^k, X^{k+1}, \ldots, X^{n-1} \). That is coefficients of these powers of \( X \) are zero. So, we get \( n - k \) equalities:

\[ \sum_{i=0}^{k} h_i v_{n-i-j} = 0 \text{ for } 1 \leq j \leq n - k. \]

So, we have \( H \) as:

![Matrix](image)

**Theorem 7:** let \( g(X) \) be the generator polynomial of the \((n, k)\) cyclic code \( C \). The dual code of \( C \) is generated by \( X^k h(X^{-1}) \) where \( h(X) = \frac{X^{n+1}}{g(X)} \).

**Example:** consider \((7, 4)\) code \( C \) with \( g(X) = 1 + X + X^3 \). The generator polynomial of \( C^t \) is \( X^4 h(X^{-1}) \) where

\[ h(X) = \frac{X^7 + 1}{1 + X + X^3} = 1 + X + X^2 + X^4. \]

That is, the generator of \( C^t \) is:

\[ X^4 h(X^{-1}) = X^4(1 + X^{-1} + X^{-2} + X^{-4}) \]
\[ = 1 + X^2 + X^3 + X^4. \]

So, \( C^t \) is a \((7, 3)\) code with \( d_{\text{min}} = 4 \). Therefore, it can correct any single error and detect any combination of double errors.

**Encoding of cyclic codes:**

We saw that if we multiply the information polynomial by \( X^{n-k} \) and divide by \( g(X) \), we get:

\[ X^{n-1} u(X) = a(X)g(X) + b(X) \]

and

\[ a(X)g(X) = b(X) + X^{n-1} u(X) \]
is a codeword in systematic form. The following circuit encodes \( u(X) \) based on the above discussion.

![Encoding circuit for an \((n, k)\) cyclic code with generator polynomial \( g(X) = 1 + g_1 X^2 + \cdots + g_{n-k-1} X^{n-k-1} + X^{n-k} \).](image)

1) Close the gate and enter information bits in and also send them over channel. This does multiplication by \( X^{n-k} \) as well as parity bit generation.
2) Open the gate (break the feedback).
3) Output the \( n-k \) parity bits.

**Example:** \((7, 4)\) code with \( g(X) = 1 + X + X^3 \).

![Encoder for the \((7, 4)\) cyclic code generated by \( g(X) = 1 + X + X^3 \).](image)

** Syndrome:**

Assume \( r(X) = r_0 + r_1 X + r_2 X^2 + \cdots + r_{n-1} X^{n-1} \) is the polynomial representing received bits. Divide \( r(X) \) by \( g(X) \) to get:

\[
 r(X) = a(X)g(X) + s(X).
\]

\( s(X) \) is a polynomial of degree \( n-k-1 \) or less. The \( n-k \) coefficients of \( s(X) \) are the syndromes.
Theorem 8: let $s(X)$ be the syndrome of $r(X) = r_0 + r_1X + \cdots + r_{n-1}X^{n-1}$. Then, $s^{(i)}(X)$ resulting from dividing $X^is(X)$ by $g(X)$ is the syndrome of $r^{(i)}(X)$.

Example of $(7, 4)$ code:

**FIGURE 5.6:** Syndrome circuit for the $(7, 4)$ cyclic code generated by $g(X) = 1 + X + X^3$.

<table>
<thead>
<tr>
<th>Shift</th>
<th>Input</th>
<th>Register contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>000 (initial state)</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>000</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>100</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>110</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>011</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>011</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>111</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>101 (syndrome s)</td>
</tr>
<tr>
<td>8</td>
<td>—</td>
<td>100 (syndrome $s^{(1)}$)</td>
</tr>
<tr>
<td>9</td>
<td>—</td>
<td>010 (syndrome $s^{(2)}$)</td>
</tr>
</tbody>
</table>

Decoding:
Example of \((7, 4)\) code:

<table>
<thead>
<tr>
<th>Error pattern (e(X))</th>
<th>Syndrome (s(X))</th>
<th>Syndrome vector ((s_0, s_1, s_2))</th>
</tr>
</thead>
<tbody>
<tr>
<td>(e_6(X) = X^6)</td>
<td>(s(X) = 1 + X^2)</td>
<td>((101))</td>
</tr>
<tr>
<td>(e_5(X) = X^5)</td>
<td>(s(X) = 1 + X + X^2)</td>
<td>((111))</td>
</tr>
<tr>
<td>(e_4(X) = X^4)</td>
<td>(s(X) = X + X^2)</td>
<td>((011))</td>
</tr>
<tr>
<td>(e_3(X) = X^3)</td>
<td>(s(X) = 1 + X)</td>
<td>((110))</td>
</tr>
<tr>
<td>(e_2(X) = X^2)</td>
<td>(s(X) = X^2)</td>
<td>((001))</td>
</tr>
<tr>
<td>(e_1(X) = X^1)</td>
<td>(s(X) = X)</td>
<td>((010))</td>
</tr>
<tr>
<td>(e_0(X) = X^0)</td>
<td>(s(X) = 1)</td>
<td>((100))</td>
</tr>
</tbody>
</table>
Another implementation of syndrome calculator

Decoding circuit for the (7, 4) cyclic code generated by $g(X) = 1 + X + X^3$.

General cyclic code decoder with received polynomial $r(X)$ shifted into the syndrome register from the right end.

Another implementation of syndrome calculator
Syndrome decoding of (7, 4) code using syndrome decoder fed from right:

<table>
<thead>
<tr>
<th>Error pattern $e(X)$</th>
<th>Syndrome $s^{(3)}(X)$</th>
<th>Syndrome vector $(s_0, s_1, s_2)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$e(X) = X^6$</td>
<td>$s^{(3)}(X) = X^2$</td>
<td>(001)</td>
</tr>
<tr>
<td>$e(X) = X^5$</td>
<td>$s^{(3)}(X) = X$</td>
<td>(010)</td>
</tr>
<tr>
<td>$e(X) = X^4$</td>
<td>$s^{(3)}(X) = 1$</td>
<td>(100)</td>
</tr>
<tr>
<td>$e(X) = X^3$</td>
<td>$s^{(3)}(X) = 1 + X^2$</td>
<td>(101)</td>
</tr>
<tr>
<td>$e(X) = X^2$</td>
<td>$s^{(3)}(X) = 1 + X + X^2$</td>
<td>(111)</td>
</tr>
<tr>
<td>$e(X) = X$</td>
<td>$s^{(3)}(X) = X + X^2$</td>
<td>(011)</td>
</tr>
<tr>
<td>$e(X) = X^0$</td>
<td>$s^{(3)}(X) = 1 + X$</td>
<td>(110)</td>
</tr>
</tbody>
</table>

**Cyclic Hamming codes:**

A Hamming code of length $n = 2^m - 1$ with $m \geq 3$ is generated by a primitive polynomial of degree $m$. Let’s see how we can put the Hamming code with defined in last lecture in cyclic form:

Divide $X^{m+i}$ by $p(X)$ to get $X^{m+i} = a_i(X)p(X) + b_i(X)$.

1) Since $p(X)$ is primitive, $X$ is not a factor of $p(X)$ so $p(X)$ does not divide $X^{m+i} \Rightarrow b_i(X) \neq 0$. 

[Diagram of decoding circuit for the (7, 4) cyclic code generated by $g(X) = 1 + X + X^3$.]

Error patterns and their syndromes with the received polynomial $r(X)$ shifted into the syndrome register from the right end.
2) \(b_i(X)\) has at least two terms. If it had one term:

\[
X^{m+i} = a_i(X)p(X) + X^l
\]

\[
\Rightarrow X^l(X^{m+i-l} + 1) = a_i(X)p(X)
\]

\[
\Rightarrow p(X) \text{ divides } X^{m+i-l} + 1 \text{ but } m + i - j < 2^m - 1
\]

\[
\Rightarrow \text{contradiction.}
\]

3) If \(i \neq j\), then \(b_i(X) \neq b_j(X)\). Let

\[
X^{m+i} = b_i(X) + a_i(X)p(X)
\]

\[
X^{m+j} = b_j(X) + a_j(X)p(X).
\]

If \(b_i(X) = b_j(X)\), then

\[
x^{m+i}(x^{j-i} + 1) = [a_i(X) + a_j(X)]p(X),
\]

i.e., \(p(X)\) divides \(X^{j-i} + 1 \Rightarrow \text{contradiction.}\)

Let \(H = [I_m: Q]\) be the parity check matrix of this code. \(I_m\) is an \(m \times m\) identity matrix with \(Q\) an \(m \times (2^m - m - 1)\) matrix with \(b_i = (b_{i0}, b_{i1}, \ldots, b_{i,m-1})\) as its columns. Since no two columns of \(Q\) are the same and each have at least two 1's, then \(H\) is indeed a parity-check matrix of a Hamming code.

** Syndrome decoding of Hamming codes:**

Assume that error is in location with highest order, i.e.,

\[
e(X) = X^{2^{m-2}}.
\]

Then, feeding \(r(X)\) from right to syndrome calculator is equivalent to dividing \(X^m \cdot X^{2^{m-2}}\) by the generator polynomial \(p(X)\). Since \(p(X)\) divides \(X^{2^{m-1}} + 1\) then

\[
s(X) = X^{m-1} \text{ or } s = (0, 0, \cdots, 0, 1).
\]