Let $GF(2^4) = GF(2)[x]/(p(x))$, where $p(x)$ is the primitive polynomial $p(x) = x^4 + x + 1$, and let $\xi$ be the primitive root $\xi = x \mod p(x)$.

We let $g(x)$ be the monic polynomial of smallest degree having the following zeroes: $\xi, \xi^2, \xi^3, \xi^4$, and let $V$ be the length 15 given by the generator polynomial $g(x)$. Hence, since $g(x)$ has four consecutive roots, $V$ is a BCH code with design distance $\delta = 4 + 1 = 5$. Hence, the minimum distance $d$ of $V$ is bounded below by $\delta$, i.e., $d \geq \delta = 5 = 2 \cdot 2 + 1 = 2t + 1$. This implies that the the BCH code $V$ is capable of correcting at least $t = 2$ errors.

Since $\xi$, $\xi^2$, and $\xi^4$ are all conjugate to each other, and since $\xi$ and $\xi^3$ are not conjugate, $g(x)$ is simply the polynomial of smallest degree having $\xi$ and $\xi^3$ as roots. Thus, the parity matrix is given by

$$H = \begin{pmatrix} \xi^{14} & \xi^{13} & \xi^{12} & \cdots & \xi^2 & \xi^1 & 1 \\ (\xi^3)^{14} & (\xi^3)^{13} & (\xi^3)^{12} & \cdots & (\xi^3)^2 & (\xi^3)^1 & 1 \end{pmatrix}$$

which simplifies to

$$H = \begin{pmatrix} \xi^{14} & \xi^{13} & \xi^{12} & \cdots & \xi^2 & \xi^1 & 1 \\ \xi^{12} & \xi^9 & \xi^6 & \cdots & \xi^6 & \xi^3 & 1 \end{pmatrix}.$$

Let us assume that a code vector $\overrightarrow{c}$ is sent over a BSC, and that the received vector is $\overrightarrow{r} = \overrightarrow{c} + \overrightarrow{e}$, where $\overrightarrow{e}$ denotes the error vector. Let us further assume that exactly two errors have occured, i.e.,

$$\overrightarrow{e} = \overrightarrow{e}_i + \overrightarrow{e}_j,$$

where $\overrightarrow{e}_i$ and $\overrightarrow{e}_j$ denote length 15 binary with 1 in the $i$-th and the $j$-th positions, respectively, and with all other entries equal to zero. Thus, we have

$$\overrightarrow{c} \xrightarrow{\text{BSC}} \overrightarrow{r} = \overrightarrow{c} + \overrightarrow{e} = \overrightarrow{r} = \overrightarrow{c} + \overrightarrow{e}_i + \overrightarrow{e}_j.$$

Let us now compute the syndrome of the received vector $\overrightarrow{r}$.

$$\text{Syn}(\overrightarrow{r}) = \text{Syn}(\overrightarrow{c})$$

Date: December 4, 2007.
If we let $\gamma_j$ denote the $j$-th column of $H$, i.e.,

$$H = \begin{pmatrix} \gamma_{14} & \gamma_{13} & \gamma_{12} & \cdots & \gamma_2 & \gamma_1 & \gamma_0 \end{pmatrix},$$

and use the fact that the error vector is of the form

$$\vec{\tau} = (0 \quad \cdots \quad 0 \quad 1 \quad 0 \quad \cdots \quad 0 \quad 1 \quad \cdots \quad 0),$$

we have

$$\text{Syn}(\vec{r}) = \begin{pmatrix} \xi_i + \xi_j \\ (\xi_i^3 + (\xi_j)^3) \end{pmatrix}.$$ 

We will call the field elements $\xi_i$ and $\xi_j$ error locators, since their logs are the locations of the two respective errors. Knowing the error locators is equivalent to knowing the error locations.

Let us denote the two components of $\text{Syn}(\vec{r})$ by $z_1$ and $z_2$, respectively. Thus,

$$\text{Syn}(\vec{r}) = \begin{pmatrix} \xi_i + \xi_j \\ (\xi_i^3 + (\xi_j)^3) \end{pmatrix} = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}.$$ 

We would now like to construct from the components $z_1$ and $z_2$ of the syndrome, the error location polynomial $S(x)$. The error location polynomial $S(x)$ is the polynomial over $GF(2^4)$ whose roots are the error locator. In other words, 

$$S(x) = (x + \xi^i)(x + \xi^j) = x^2 + (\xi^i + \xi^j)x + (\xi^i \cdot \xi^j)$$

Since

$$\begin{cases} \xi^i + \xi^j = z_1 \\ (\xi^i)^3 + (\xi^j)^3 = z_2 \end{cases},$$

we have

$$z_2 = (\xi^i + \xi^j)(\xi^i)^2 + \xi^i \xi^j = z_1 (z_1^2 + (\xi^i)^2).$$

Hence,

$$\xi^i \xi^j = \frac{z_2}{z_1} + z_1^2.$$ 

Thus,

$$S(x) = (x + \xi^i)(x + \xi^j) = S(x) = (x + \xi^i)(x + \xi^j) = x^2 + z_1 x + \left(\frac{z_2}{z_1} + z_1^2\right)$$

Thus, the error locators can be found simply by finding the roots of the above error locator polynomial (which was computed from the syndrome of the received vector.)

Given the syndrome $\text{Syn}(\vec{r}) = (z_1, z_2)^T$ of the received vector $\vec{r}$, our error correcting scheme is as follows:

i) If $z_1 = z_2 = 0$, then we decide that no error has occurred.
ii) If \( z_1 \neq 0 \) and \( z_2 = z_3 \), then we decide that a single error has occurred at the error locator \( z_1 = \xi^i \).

iii) If \( z_1 \neq 0 \) and \( z_2 \neq z_3 \), then we decide that two errors have occurred, and we find the two error locators \( \xi^i \) and \( \xi^j \) by finding the two roots of the error locator polynomial \( S(x) \).

**Example 1.** As an example, let consider the case when two errors have occurred at locations 6 and 8. We will use the attached AntiLog/Log table for our calculations.

The syndrome of the received vector \( \vec{r} \)

\[
\text{Syn}(\vec{r}) = \begin{pmatrix}
\xi^6 + \xi^8 \\
(\xi^6)^3 + (\xi^6)^3
\end{pmatrix} = \begin{pmatrix}
\xi^6 + \xi^8 \\
\xi^3 + \xi^9
\end{pmatrix} = \begin{pmatrix}
\xi^{14} \\
\xi
\end{pmatrix} = \begin{pmatrix}
z_1 \\
z_2
\end{pmatrix}
\]

Since,

\[
\frac{z_2}{z_1} + z_1 = \frac{\xi}{\xi^{14}} + (\xi^{14})^2 = \xi^2 + \xi^{13} = \xi^{14},
\]

the error locator polynomial is

\[
S(x) = x^2 + \xi^{14}x + \xi^{14}
\]

One can easily check that

\[
S(x) = x^2 + \xi^{14}x + \xi^{14} = (x + \xi^6)(x + \xi^8)
\]

**Problem 1.** If the received vector \( \vec{r} \) is

\[
\vec{r} = 10110 00101 11100
\]

compute the syndrome \( \text{Syn}(\vec{r}) \), and the error locator polynomial \( S(x) \). Once you have the error locator polynomial \( S(x) \) use it to find the two error locators \( \xi^i \) and \( \xi^j \), and the corrected code vector.

**References**


\[ p(x) = x^4 + x + 1 \]

<table>
<thead>
<tr>
<th>AntiLog</th>
<th>Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000</td>
<td>(-\infty)</td>
</tr>
<tr>
<td>1000</td>
<td>0</td>
</tr>
<tr>
<td>0100</td>
<td>1</td>
</tr>
<tr>
<td>0010</td>
<td>2</td>
</tr>
<tr>
<td>0001</td>
<td>3</td>
</tr>
<tr>
<td>1100</td>
<td>4</td>
</tr>
<tr>
<td>0110</td>
<td>5</td>
</tr>
<tr>
<td>0011</td>
<td>6</td>
</tr>
<tr>
<td>1101</td>
<td>7</td>
</tr>
<tr>
<td>1010</td>
<td>8</td>
</tr>
<tr>
<td>0101</td>
<td>9</td>
</tr>
<tr>
<td>1110</td>
<td>10</td>
</tr>
<tr>
<td>0111</td>
<td>11</td>
</tr>
<tr>
<td>1111</td>
<td>12</td>
</tr>
<tr>
<td>1011</td>
<td>13</td>
</tr>
<tr>
<td>1001</td>
<td>14</td>
</tr>
</tbody>
</table>