BCH Codes

Yunghsiang S. Han

Graduate Institute of Communication Engineering, National Taipei University, Taiwan
E-mail: yshan@mail.ntpu.edu.tw
Description of BCH Codes

- The Bose, Chaudhuri, and Hocquenghem (BCH) codes form a large class of powerful random error-correcting cyclic codes.
- This class of codes is a remarkable generalization of the Hamming code for multiple-error correction.
- We only consider binary BCH codes in this lecture note. Non-binary BCH codes such as Reed-Solomon codes will be discussed in next lecture note.
- For any positive integers $m \geq 3$ and $t < 2^{m-1}$, there exists a binary BCH code with the following parameters:

  - Block length: $n = 2^m - 1$
  - Number of parity-check digits: $n - k \leq mt$
  - Minimum distance: $d_{min} \geq 2t + 1$. 

Graduate Institute of Communication Engineering, National Taipei University
• We call this code a \textit{t-error-correcting} BCH code.

• Let $\alpha$ be a primitive element in $GF(2^m)$. The generator polynomial $g(x)$ of the $t$-error-correcting BCH code of length $2^m - 1$ is the \textit{lowest-degree polynomial} over $GF(2)$ which has $\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{2t}$ as its roots.

• $g(\alpha^i) = 0$ for $1 \leq i \leq 2t$ and $g(x)$ has $\alpha, \alpha^2, \ldots, \alpha^{2t}$ and their conjugates as all its roots.

• Let $\phi_i(x)$ be the minimal polynomial of $\alpha^i$. Then $g(x)$ must be the \textit{least common multiple} of $\phi_1(x), \phi_2(x), \ldots, \phi_{2t}(x)$, i.e.,

$$g(x) = \text{LCM}\{\phi_1(x), \phi_2(x), \ldots, \phi(x)_{2t}\}.$$ 

• If $i$ is an even integer, it can be expressed as $i = i'2^\ell$, where $i'$ is
odd and $\ell > 1$. Then $\alpha^i = \left(\alpha^{i'}\right)^{2^\ell}$ is a conjugate of $\alpha^{i'}$. Hence, $\phi_i(x) = \phi_{i'}(x)$.

- $g(x) = \text{LCM}\{\phi_1(x), \phi_3(x), \ldots, \phi_{2t-1}(x)\}$.

- The degree of $g(x)$ is at most $mt$. That is, the number of parity-check digits, $n - k$, of the code is at most equal to $mt$.

- If $t$ is small, $n - k$ is exactly equal to $mt$.

- Since $\alpha$ is a primitive element, the BCH codes defined are usually called primitive (or narrow-sense) BCH codes.
Example

- Let \( \alpha \) be a primitive element of \( GF(2^4) \) such that \( 1 + \alpha + \alpha^4 = 0 \). The minimal polynomials of \( \alpha, \alpha^3, \) and \( \alpha^5 \) are

\[
\begin{align*}
\phi_1(x) & = 1 + x + x^4, \\
\phi_3(x) & = 1 + x + x^2 + x^3 + x^4, \\
\phi_5(x) & = 1 + x + x^2,
\end{align*}
\]

respectively. The double-error-correcting BCH code of length \( n = 2^4 - 1 = 15 \) is generated by

\[
g(x) = \text{LCM}\{\phi_1(x), \phi_3(x)\} = (1 + x + x^4)(1 + x + x^2 + x^3 + x^4)
\]

\[
= 1 + x^4 + x^6 + x^7 + x^8.
\]

\( n - k = 8 \) such that this is a \( (15, 7, \geq 5) \) code. Since the weight of
the generator polynomial is 5, it is a \((15, 7, 5)\) code.

- The triple-error-correcting BCH code of length 15 is generated by

\[
g(x) = \text{LCM}\{\phi_1(x), \phi_3(x), \phi_5(x)\} \\
= (1 + x + x^4)(1 + x + x^2 + x^3 + x^4)(1 + x + x^2) \\
= 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}.
\]

\(n - k = 10\) such that this is a \((15, 5, \geq 7)\) code. Since the weight of the generator polynomial is 7, it is a \((15, 5, 7)\) code.

- The single-error-correcting BCH code of length \(2^m - 1\) is a Hamming code.
\begin{table}
\centering
\begin{tabular}{|c|c|c|c|c|}
\hline
Exponential Notation & Polynomial Notation & Binary Notation & Decimal Notation & Minimal Polynomial \\
\hline
0 & 0 & 0000 & 0 & x \\
\hline
\(\alpha^0\) & 1 & 0001 & 1 & \(x + 1\) \\
\hline
\(\alpha^1\) & z & 0010 & 2 & \(x^4 + x + 1\) \\
\hline
\(\alpha^2\) & \(z^2\) & 0100 & 4 & \(x^4 + x + 1\) \\
\hline
\(\alpha^3\) & \(z^3\) & 1000 & 8 & \(x^4 + x^3 + x^2 + x + 1\) \\
\hline
\(\alpha^4\) & \(z + 1\) & 0011 & 3 & \(x^4 + x + 1\) \\
\hline
\(\alpha^5\) & \(z^2 + z\) & 0110 & 6 & \(x^2 + x + 1\) \\
\hline
\(\alpha^6\) & \(z^3 + z^2\) & 1100 & 12 & \(x^4 + x^3 + x^2 + x + 1\) \\
\hline
\(\alpha^7\) & \(z^3 + z + 1\) & 1011 & 11 & \(x^4 + x^3 + 1\) \\
\hline
\(\alpha^8\) & \(z^2 + 1\) & 0101 & 5 & \(x^4 + x + 1\) \\
\hline
\(\alpha^9\) & \(z^3 + z\) & 1010 & 10 & \(x^4 + x^3 + x^2 + x + 1\) \\
\hline
\(\alpha^{10}\) & \(z^2 + z + 1\) & 0111 & 7 & \(x^2 + x + 1\) \\
\hline
\(\alpha^{11}\) & \(z^3 + z^2 + z + 1\) & 1110 & 14 & \(x^4 + x^3 + 1\) \\
\hline
\(\alpha^{12}\) & \(z^3 + z^2 + z + 1\) & 1111 & 15 & \(x^4 + x^3 + x^2 + x + 1\) \\
\hline
\(\alpha^{13}\) & \(z^3 + z^2 + 1\) & 1101 & 13 & \(x^4 + x^3 + 1\) \\
\hline
\(\alpha^{14}\) & \(z^3 + 1\) & 1001 & 9 & \(x^4 + x^3 + 1\) \\
\hline
\end{tabular}
\end{table}

\(\alpha \alpha^2 \alpha^4 \alpha^8 \alpha^{16} \equiv \alpha\)

\(\alpha^3 \alpha^6 \alpha^{12} \alpha^{24} \alpha^{48} \equiv \alpha^3 \equiv \alpha^9\)
Examples of Finite Fields

\[ \begin{array}{c|cccc} + & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 1 & 2 & 3 \\ 1 & 1 & 0 & 3 & 2 \\ 2 & 2 & 3 & 0 & 1 \\ 3 & 3 & 2 & 1 & 0 \end{array} \]

\[ \begin{array}{c|cccc} \cdot & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 & 3 \\ 2 & 0 & 2 & 3 & 1 \\ 3 & 0 & 3 & 1 & 2 \end{array} \]

\[ \text{GF}(4)^2 = \text{GF}(4)[z]/z^2+z+2, \ p(z) = z^2+z+2 \]

\[ \alpha = z \]
\[ \alpha^{15} = 1 \]
BCH Codes of Lengths Less than $2^{10} - 1$ (1)

<table>
<thead>
<tr>
<th>m</th>
<th>n</th>
<th>k</th>
<th>t</th>
<th>m</th>
<th>n</th>
<th>k</th>
<th>t</th>
<th>m</th>
<th>n</th>
<th>k</th>
<th>t</th>
<th>n</th>
<th>k</th>
<th>t</th>
<th>n</th>
<th>k</th>
<th>t</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>7</td>
<td>4</td>
<td>1</td>
<td>63</td>
<td>24</td>
<td>7</td>
<td></td>
<td>127</td>
<td>50</td>
<td>13</td>
<td></td>
<td>255</td>
<td>187</td>
<td>9</td>
<td></td>
<td>255</td>
<td>71</td>
</tr>
<tr>
<td>4</td>
<td>15</td>
<td>11</td>
<td>1</td>
<td>18</td>
<td>10</td>
<td>43</td>
<td>14</td>
<td>179</td>
<td>10</td>
<td>63</td>
<td>30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>2</td>
<td></td>
<td></td>
<td>16</td>
<td>11</td>
<td>36</td>
<td>15</td>
<td>171</td>
<td>11</td>
<td>55</td>
<td>31</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td></td>
<td></td>
<td>40</td>
<td>13</td>
<td>29</td>
<td>21</td>
<td>163</td>
<td>12</td>
<td>47</td>
<td>42</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>31</td>
<td>26</td>
<td>1</td>
<td>7</td>
<td>15</td>
<td>22</td>
<td>23</td>
<td>155</td>
<td>13</td>
<td>45</td>
<td>43</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>2</td>
<td></td>
<td></td>
<td>120</td>
<td>1</td>
<td>15</td>
<td>27</td>
<td>147</td>
<td>14</td>
<td>37</td>
<td>45</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>3</td>
<td></td>
<td></td>
<td>113</td>
<td>2</td>
<td>8</td>
<td>31</td>
<td>139</td>
<td>15</td>
<td>29</td>
<td>47</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>5</td>
<td></td>
<td></td>
<td>106</td>
<td>3</td>
<td>255</td>
<td>247</td>
<td>131</td>
<td>18</td>
<td>21</td>
<td>55</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>7</td>
<td></td>
<td></td>
<td>99</td>
<td>4</td>
<td>239</td>
<td>2</td>
<td>123</td>
<td>19</td>
<td>13</td>
<td>59</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>63</td>
<td>57</td>
<td>1</td>
<td>92</td>
<td>5</td>
<td>231</td>
<td>3</td>
<td>115</td>
<td>21</td>
<td>9</td>
<td>63</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>51</td>
<td></td>
<td></td>
<td></td>
<td>85</td>
<td>6</td>
<td>223</td>
<td>4</td>
<td>107</td>
<td>22</td>
<td>511</td>
<td>502</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>45</td>
<td>3</td>
<td></td>
<td></td>
<td>78</td>
<td>7</td>
<td>215</td>
<td>5</td>
<td>99</td>
<td>23</td>
<td>493</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>39</td>
<td>4</td>
<td></td>
<td></td>
<td>71</td>
<td>9</td>
<td>207</td>
<td>6</td>
<td>91</td>
<td>25</td>
<td>484</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>5</td>
<td></td>
<td></td>
<td>64</td>
<td>10</td>
<td>199</td>
<td>7</td>
<td>87</td>
<td>26</td>
<td>475</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>6</td>
<td></td>
<td></td>
<td>57</td>
<td>11</td>
<td>191</td>
<td>8</td>
<td>79</td>
<td>27</td>
<td>466</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For $t$ small
$n - k = mt$
### BCH Codes of Lengths Less than $2^{10} - 1$ (2)

<table>
<thead>
<tr>
<th>n</th>
<th>k</th>
<th>t</th>
<th>n</th>
<th>k</th>
<th>t</th>
<th>n</th>
<th>k</th>
<th>t</th>
<th>n</th>
<th>k</th>
<th>t</th>
</tr>
</thead>
<tbody>
<tr>
<td>511</td>
<td>457</td>
<td>6</td>
<td>511</td>
<td>322</td>
<td>22</td>
<td>511</td>
<td>193</td>
<td>43</td>
<td>511</td>
<td>58</td>
<td>91</td>
</tr>
<tr>
<td>448</td>
<td>7</td>
<td>313</td>
<td>23</td>
<td>184</td>
<td>45</td>
<td>49</td>
<td>93</td>
<td>923</td>
<td>10</td>
<td>913</td>
<td>11</td>
</tr>
<tr>
<td>439</td>
<td>8</td>
<td>304</td>
<td>25</td>
<td>175</td>
<td>46</td>
<td>40</td>
<td>95</td>
<td>903</td>
<td>12</td>
<td>893</td>
<td>13</td>
</tr>
<tr>
<td>430</td>
<td>9</td>
<td>295</td>
<td>26</td>
<td>166</td>
<td>47</td>
<td>31</td>
<td>109</td>
<td>903</td>
<td>12</td>
<td>893</td>
<td>13</td>
</tr>
<tr>
<td>421</td>
<td>10</td>
<td>286</td>
<td>27</td>
<td>157</td>
<td>51</td>
<td>28</td>
<td>111</td>
<td>893</td>
<td>13</td>
<td>883</td>
<td>14</td>
</tr>
<tr>
<td>412</td>
<td>11</td>
<td>277</td>
<td>28</td>
<td>148</td>
<td>53</td>
<td>19</td>
<td>119</td>
<td>883</td>
<td>14</td>
<td>873</td>
<td>15</td>
</tr>
<tr>
<td>403</td>
<td>12</td>
<td>268</td>
<td>29</td>
<td>139</td>
<td>54</td>
<td>10</td>
<td>121</td>
<td>873</td>
<td>15</td>
<td>863</td>
<td>16</td>
</tr>
<tr>
<td>394</td>
<td>13</td>
<td>259</td>
<td>30</td>
<td>130</td>
<td>55</td>
<td>1013</td>
<td>1</td>
<td>863</td>
<td>16</td>
<td>858</td>
<td>17</td>
</tr>
<tr>
<td>385</td>
<td>14</td>
<td>250</td>
<td>31</td>
<td>121</td>
<td>58</td>
<td>1023</td>
<td>1003</td>
<td>2</td>
<td>858</td>
<td>17</td>
<td></td>
</tr>
<tr>
<td>376</td>
<td>15</td>
<td>241</td>
<td>36</td>
<td>112</td>
<td>59</td>
<td>993</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>367</td>
<td>16</td>
<td>238</td>
<td>37</td>
<td>103</td>
<td>61</td>
<td>983</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>358</td>
<td>18</td>
<td>229</td>
<td>38</td>
<td>94</td>
<td>62</td>
<td>973</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>349</td>
<td>19</td>
<td>220</td>
<td>39</td>
<td>85</td>
<td>63</td>
<td>963</td>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>340</td>
<td>20</td>
<td>211</td>
<td>41</td>
<td>76</td>
<td>85</td>
<td>953</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>331</td>
<td>21</td>
<td>202</td>
<td>42</td>
<td>67</td>
<td>87</td>
<td>943</td>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( \alpha )</td>
<td>( \alpha^2 )</td>
<td>( \alpha^3 )</td>
<td>( \alpha^4 )</td>
<td>( \alpha^5 )</td>
<td>( \alpha^6 )</td>
<td>( \alpha^7 )</td>
<td>( \alpha^8 )</td>
<td>( \alpha^9 )</td>
<td>( \alpha^{10} )</td>
<td>( \alpha^{11} )</td>
<td>( \alpha^{12} )</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>(0 0 0 0 0 0)</td>
<td>( \alpha^{15} )</td>
<td>( \alpha^3 )</td>
<td>+( \alpha^5 )</td>
<td>(0 0 0 1 0 1)</td>
<td>( \alpha^{17} )</td>
<td>( \alpha+\alpha^2 )</td>
<td>+( \alpha^5 )</td>
<td>(0 1 1 0 0 1)</td>
<td>( \alpha^{18} )</td>
</tr>
<tr>
<td>$\alpha^3$</td>
<td>1</td>
<td>$+\alpha^2$</td>
<td>$+\alpha^5$</td>
<td>(1 0 1 0 0 1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\alpha^3$</td>
<td>1</td>
<td>$+\alpha^3$</td>
<td>(1 0 0 1 0 0)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\alpha^3$</td>
<td>$\alpha$</td>
<td>$+\alpha^4$</td>
<td>(0 1 0 0 1 0)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\alpha^3$</td>
<td>$\alpha^2$</td>
<td>$+\alpha^5$</td>
<td>(0 0 1 0 0 1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\alpha^3$</td>
<td>$1+\alpha$</td>
<td>$+\alpha^3$</td>
<td>(1 1 0 1 0 0)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\alpha^3$</td>
<td>$\alpha+\alpha^2$</td>
<td>$+\alpha^4$</td>
<td>(0 1 1 0 1 0)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\alpha^3$</td>
<td>$\alpha^2+\alpha^3$</td>
<td>$+\alpha^5$</td>
<td>(0 0 1 1 0 1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\alpha^3$</td>
<td>$1+\alpha$</td>
<td>$+\alpha^3+\alpha^4$</td>
<td>(1 1 0 1 1 0)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\alpha^3$</td>
<td>$\alpha+\alpha^2$</td>
<td>$+\alpha^3+\alpha^4$</td>
<td>(0 1 1 0 1 1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\alpha^3$</td>
<td>$1+\alpha+\alpha^2+\alpha^3$</td>
<td>$+\alpha^5$</td>
<td>(1 1 1 0 1 1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\alpha^3$</td>
<td>1</td>
<td>$+\alpha^2+\alpha^3+\alpha^4$</td>
<td>(1 0 1 1 1 0)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\alpha^3$</td>
<td>$\alpha+\alpha^3+\alpha^4+\alpha^5$</td>
<td>(0 1 0 1 1 1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\alpha^3$</td>
<td>$1+\alpha+\alpha^2$</td>
<td>$+\alpha^4+\alpha^5$</td>
<td>(1 1 1 0 1 1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\alpha^3$</td>
<td>$\alpha+\alpha^2+\alpha^3+\alpha^4+\alpha^5$</td>
<td>(1 1 1 1 1 1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\alpha^3$</td>
<td>$1+\alpha+\alpha^2+\alpha^3+\alpha^4+\alpha^5$</td>
<td>(1 1 1 1 1 1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\alpha^3$</td>
<td>$\alpha+\alpha^2+\alpha^3+\alpha^4+\alpha^5$</td>
<td>(1 0 1 1 1 1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\alpha^3$</td>
<td>$1+\alpha+\alpha^2+\alpha^3+\alpha^4+\alpha^5$</td>
<td>(1 0 0 1 1 1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\alpha^3$</td>
<td>$\alpha+\alpha^2+\alpha^3+\alpha^4+\alpha^5$</td>
<td>(1 0 0 0 1 1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\alpha^3$</td>
<td>$\alpha+\alpha^2+\alpha^3+\alpha^4+\alpha^5$</td>
<td>(1 0 0 0 1 1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Minimal Polynomials of the Elements in $GF(2^6)$

<table>
<thead>
<tr>
<th>Elements</th>
<th>Minimal polynomials</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\alpha$, $\alpha^2$, $\alpha^4$, $\alpha^8$, $\alpha^{16}$, $\alpha^{32}$</td>
<td>$1 + \alpha + \alpha^6$</td>
</tr>
<tr>
<td>$\alpha^3$, $\alpha^6$, $\alpha^{12}$, $\alpha^{24}$, $\alpha^{48}$, $\alpha^{33}$</td>
<td>$1 + \alpha + \alpha^2 + \alpha^4 + \alpha^6$</td>
</tr>
<tr>
<td>$\alpha^5$, $\alpha^{10}$, $\alpha^{20}$, $\alpha^{40}$, $\alpha^{17}$, $\alpha^{34}$</td>
<td>$1 + \alpha + \alpha^2 + \alpha^5 + \alpha^6$</td>
</tr>
<tr>
<td>$\alpha^7$, $\alpha^{14}$, $\alpha^{28}$, $\alpha^{56}$, $\alpha^{49}$, $\alpha^{35}$</td>
<td>$1 + \alpha^3 + \alpha^6$</td>
</tr>
<tr>
<td>$\alpha^9$, $\alpha^{18}$, $\alpha^{36}$</td>
<td>$1 + \alpha^2 + \alpha^3$</td>
</tr>
<tr>
<td>$\alpha^{11}$, $\alpha^{22}$, $\alpha^{44}$, $\alpha^{25}$, $\alpha^{50}$, $\alpha^{37}$</td>
<td>$1 + \alpha^2 + \alpha^3 + \alpha^5 + \alpha^6$</td>
</tr>
<tr>
<td>$\alpha^{13}$, $\alpha^{26}$, $\alpha^{52}$, $\alpha^{41}$, $\alpha^{19}$, $\alpha^{38}$</td>
<td>$1 + \alpha + \alpha^3 + \alpha^4 + \alpha^6$</td>
</tr>
<tr>
<td>$\alpha^{15}$, $\alpha^{30}$, $\alpha^{60}$, $\alpha^{57}$, $\alpha^{51}$, $\alpha^{39}$</td>
<td>$1 + \alpha^2 + \alpha^4 + \alpha^5 + \alpha^6$</td>
</tr>
<tr>
<td>$\alpha^{21}$, $\alpha^{42}$</td>
<td>$1 + \alpha + \alpha^2$</td>
</tr>
<tr>
<td>$\alpha^{23}$, $\alpha^{46}$, $\alpha^{29}$, $\alpha^{58}$, $\alpha^{53}$, $\alpha^{43}$</td>
<td>$1 + \alpha + \alpha^4 + \alpha^5 + \alpha^6$</td>
</tr>
<tr>
<td>$\alpha^{27}$, $\alpha^{54}$, $\alpha^{45}$</td>
<td>$1 + \alpha + \alpha^6$</td>
</tr>
<tr>
<td>$\alpha^{31}$, $\alpha^{62}$, $\alpha^{61}$, $\alpha^{59}$, $\alpha^{55}$, $\alpha^{47}$</td>
<td>$1 + \alpha^5 + \alpha^6$</td>
</tr>
</tbody>
</table>
Generator Polynomials of All BCH Codes of Length 63

<table>
<thead>
<tr>
<th>n</th>
<th>k</th>
<th>t</th>
<th>g(X)</th>
</tr>
</thead>
<tbody>
<tr>
<td>63</td>
<td>57</td>
<td>1</td>
<td>(g_1(X) = 1 + X + X^6)</td>
</tr>
<tr>
<td>51</td>
<td>2</td>
<td>2</td>
<td>(g_2(X) = (1 + X + X^5)(1 + X + X^2 + X^4 + X^6))</td>
</tr>
<tr>
<td>45</td>
<td>3</td>
<td>3</td>
<td>(g_3(X) = (1 + X + X^2 + X^5 + X^6)g_2(X))</td>
</tr>
<tr>
<td>39</td>
<td>4</td>
<td>4</td>
<td>(g_4(X) = (1 + X^3 + X^6)g_3(X))</td>
</tr>
<tr>
<td>36</td>
<td>5</td>
<td>5</td>
<td>(g_5(X) = (1 + X^2 + X^3)g_4(X))</td>
</tr>
<tr>
<td>30</td>
<td>6</td>
<td>6</td>
<td>(g_6(X) = (1 + X^2 + X^3 + X^5 + X^6)g_5(X))</td>
</tr>
<tr>
<td>24</td>
<td>7</td>
<td>7</td>
<td>(g_7(X) = (1 + X + X^3 + X^4 + X^6)g_6(X))</td>
</tr>
<tr>
<td>18</td>
<td>10</td>
<td>10</td>
<td>(g_{10}(X) = (1 + X^2 + X^4 + X^5 + X^6)g_7(X))</td>
</tr>
<tr>
<td>16</td>
<td>11</td>
<td>11</td>
<td>(g_{11}(X) = (1 + X + X^2)g_{10}(X))</td>
</tr>
<tr>
<td>10</td>
<td>13</td>
<td>13</td>
<td>(g_{13}(X) = (1 + X + X^4 + X^5 + X^6)g_{11}(X))</td>
</tr>
<tr>
<td>7</td>
<td>15</td>
<td>15</td>
<td>(g_{15}(X) = (1 + X + X^3)g_{13}(X))</td>
</tr>
</tbody>
</table>
Parity-Check Matrix of a BCH Code

• We can define a $t$-error-correcting BCH code of length $n = 2^m - 1$ in the following manner: A binary $n$-tuple $v = (v_0, v_1, \ldots, v_{n-1})$ is a code word if and only if the polynomial $v(x) = v_0 + v_1 x + \cdots + v_{n-1} x^{n-1}$ has $\alpha, \alpha^2, \ldots, \alpha^{2t}$ as roots.

• Since $\alpha^i$ is a root of $v(x)$ for $1 \leq i \leq 2t$, then

$$v(\alpha^i) = v_0 + v_1 \alpha^i + v_2 \alpha^{2i} + \cdots + v_{n-1} \alpha^{(n-1)i} = 0.$$
• This equality can be written as a matrix product as follows:

\[
\begin{pmatrix}
1 \\
\alpha^i \\
\alpha^{2i} \\
\vdots \\
\alpha^{(n-1)i}
\end{pmatrix}
(v_0, v_1, \ldots, v_{n-1}) = 0
\]

for 1 ≤ i ≤ 2t.
• Let
\[
H = \begin{bmatrix}
1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{n-1} \\
1 & (\alpha^2) & (\alpha^2)^2 & (\alpha^2)^3 & \cdots & (\alpha^2)^{n-1} \\
1 & (\alpha^3) & (\alpha^3)^2 & (\alpha^3)^3 & \cdots & (\alpha^3)^{n-1} \\
\vdots & & & & & \\
1 & (\alpha^{2t}) & (\alpha^{2t})^2 & (\alpha^{2t})^3 & \cdots & (\alpha^{2t})^{n-1}
\end{bmatrix}.
\] (2)

• From (1), if \( \mathbf{v} = (v_0, v_1, \ldots, v_{n-1}) \) is a code word in the \( t \)-error-correcting BCH code, then
\[
\mathbf{v} \cdot H^T = 0.
\]

• If an \( n \)-tuple \( \mathbf{v} \) satisfies the above condition, \( \alpha^i \) is a root of the polynomial \( \mathbf{v}(x) \). Therefore, \( \mathbf{v} \) must be a code word in the \( t \)-error-correcting BCH code.
• \( H \) is a parity-check matrix of the code.

• If for some \( i \) and \( j \), \( \alpha^j \) is a conjugate of \( \alpha^i \), then \( v(\alpha^j) = 0 \) if and only if \( v(\alpha^i) = 0 \).

• The \( H \) matrix can be reduced to

\[
H = \begin{bmatrix}
1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{n-1} \\
1 & (\alpha^3) & (\alpha^3)^2 & (\alpha^3)^3 & \cdots & (\alpha^3)^{n-1} \\
1 & (\alpha^5) & (\alpha^5)^2 & (\alpha^5)^3 & \cdots & (\alpha^5)^{n-1} \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
1 & (\alpha^{2t-1}) & (\alpha^{2t-1})^2 & (\alpha^{2t-1})^3 & \cdots & (\alpha^{2t-1})^{n-1}
\end{bmatrix}.
\]

• If each entry of \( H \) is replaced by its corresponding \( m \)-tuple over \( GF(2) \) arranged in column form, we obtain a binary parity-check matrix for the code.
BCH Bound

• The \( t \)-error-correcting BCH code defined has minimum distance at least \( 2t + 1 \).

**Proof:** We need to show that no \( 2t \) of fewer columns of \( H \) sum to zero. Suppose that there exists a nonzero code vector \( v \) with weight \( \delta \leq 2t \). Let \( v_{j_1}, v_{j_2}, \ldots, v_{j_\delta} \) be the nonzero components of \( v \). Then

\[
0 = v \cdot H^T = (v_{j_1}, v_{j_2}, \ldots, v_{j_\delta}) \cdot \begin{bmatrix}
\alpha^{j_1} (\alpha^2)^{j_1} & \cdots & (\alpha^{2t})^{j_1} \\
\alpha^{j_2} (\alpha^2)^{j_2} & \cdots & (\alpha^{2t})^{j_2} \\
\alpha^{j_3} (\alpha^2)^{j_3} & \cdots & (\alpha^{2t})^{j_3} \\
\vdots & \vdots & \vdots \\
\alpha^{j_\delta} (\alpha^2)^{j_\delta} & \cdots & (\alpha^{2t})^{j_\delta}
\end{bmatrix}
\]
The equality above implies the following equality:

\[
(1, 1, \ldots, 1) \cdot \begin{bmatrix}
\alpha^j_1 & (\alpha^j_1)^2 & \cdots & (\alpha^j_1)^{2t} \\
\alpha^j_2 & (\alpha^j_2)^2 & \cdots & (\alpha^j_2)^{2t} \\
\alpha^j_3 & (\alpha^j_3)^2 & \cdots & (\alpha^j_3)^{2t} \\
\vdots & \vdots & \ddots & \vdots \\
\alpha^j_\delta & (\alpha^j_\delta)^2 & \cdots & (\alpha^j_\delta)^{2t}
\end{bmatrix} = \mathbf{0},
\]
which the second matrix on the left is a $\delta \times \delta$ square matrix. To satisfy the above equality, the determinant of the $\delta \times \delta$ matrix must be zero. That is,

\[
\begin{vmatrix}
\alpha^{j_1} & (\alpha^{j_1})^2 & \ldots & (\alpha^{j_1})^\delta \\
\alpha^{j_2} & (\alpha^{j_2})^2 & \ldots & (\alpha^{j_2})^\delta \\
\alpha^{j_3} & (\alpha^{j_3})^2 & \ldots & (\alpha^{j_3})^\delta \\
\vdots & \vdots & \ddots & \vdots \\
\alpha^{j_\delta} & (\alpha^{j_\delta})^2 & \ldots & (\alpha^{j_\delta})^\delta 
\end{vmatrix} = 0.
\]
Then

\[
\alpha^{j_1 + j_2 + \cdots + j_\delta} \cdot \begin{vmatrix}
1 & \alpha^{j_1} & \cdots & \alpha^{j_1(\delta-1)} \\
1 & \alpha^{j_2} & \cdots & \alpha^{j_2(\delta-1)} \\
\vdots & \vdots & \ddots & \vdots \\
1 & \alpha^{j_\delta} & \cdots & \alpha^{j_\delta(\delta-1)}
\end{vmatrix} = 0.
\]

The determinant in the equality above is a Vandermonde determinant which is nonzero. Contradiction!

- The parameter \(2t + 1\) is usually called the designed distance of the \(t\)-error-correcting BCH code.
- The true minimum distance of the code might be larger than \(2t + 1\).
Syndrome Calculation

• Let

\[ \mathbf{r}(x) = r_0 + r_1 x + r_2 x^2 + \cdots + r_{n-1} x^{n-1} \]

be the received vector and \( e(x) \) the error pattern. Then

\[ \mathbf{r}(x) = \mathbf{v}(x) + e(x). \]

• The syndrome is a \( 2t \)-tuple,

\[ \mathbf{S} = (S_1, S_2, \ldots, S_{2t}) = \mathbf{r} \cdot \mathbf{H}^T, \]

where \( \mathbf{H} \) is given by (2).

•

\[ S_i = \mathbf{r}(\alpha^i) = r_0 + r_1 \alpha^i + r_2 \alpha^{2i} + \cdots + r_{n-1} \alpha^{(n-1)i} \]

for \( 1 \leq i \leq 2t \).
• Dividing \( r(x) \) by the minimal polynomial \( \phi_i(x) \) of \( \alpha_i \), we have

\[
r(x) = a_i(x)\phi_i(x) + b_i(x),
\]

where \( b_i(x) \) is the remainder with degree less than that of \( \phi_i(x) \).

• Since \( \phi_i(\alpha^i) = 0 \), we have

\[
S_i = r(\alpha^i) = b_i(\alpha^i).
\]

• Since \( \alpha^1, \alpha^2, \ldots, \alpha^{2t} \) are roots of each code polynomial, \( v(\alpha^i) = 0 \) for \( 1 \leq i \leq 2t \).

• Then \( S_i = e(\alpha^i) \) for \( 1 \leq i \leq 2t \).

• We now consider a general case that is also good for non-binary case.

• Suppose that the error pattern \( e(x) \) has \( v \) errors at locations
0 ≤ j_1 < j_2 < ⋯ < j_v ≤ n. That is,

\[ e(x) = e_{j_1}x^{j_1} + e_{j_2}x^{j_2} + \cdots + e_{j_v}x^{j_v}. \]

- \[ S_1 = e_{j_1}\alpha^{j_1} + e_{j_2}\alpha^{j_2} + \cdots + e_{j_v}\alpha^{j_v} \]
- \[ S_2 = e_{j_1}(\alpha^{j_1})^2 + e_{j_2}(\alpha^{j_2})^2 + \cdots + e_{j_v}(\alpha^{j_v})^2 \]
- \[ S_3 = e_{j_1}(\alpha^{j_1})^3 + e_{j_2}(\alpha^{j_2})^3 + \cdots + e_{j_v}(\alpha^{j_v})^3 \]
- \[ \vdots \]
- \[ S_{2t} = e_{j_1}(\alpha^{j_1})^{2t} + e_{j_2}(\alpha^{j_2})^{2t} + \cdots + e_{j_v}(\alpha^{j_v})^{2t}, \quad (3) \]

where \( e_{j_1}, e_{j_2}, \ldots, e_{j_v} \) and \( \alpha^{j_1}, \alpha^{j_2}, \ldots, \alpha^{j_v} \) are unknown.

- Any method for solving these equations is a decoding algorithm for the BCH codes.
- Let \( Y_i = e_{j_i}, \ X_i = \alpha^{j_i}, \ 1 ≤ i ≤ v. \)
• (3) can be rewritten as follows:

\[
\begin{align*}
S_1 &= Y_1X_1 + Y_2X_2 + \cdots + Y_vX_v \\
S_2 &= Y_1X_1^2 + Y_2X_2^2 + \cdots + Y_vX_v^2 \\
S_3 &= Y_1X_1^3 + Y_2X_2^3 + \cdots + Y_vX_v^3 \\
&\vdots \\
S_{2t} &= Y_1X_1^{2t} + Y_2X_2^{2t} + \cdots + Y_vX_v^{2t}.
\end{align*}
\]

(4)

• We need to transfer the above set of non-linear equations into a set of linear equations.

• Consider the error-locator polynomial

\[
\Lambda(x) = (1 - X_1x)(1 - X_2x) \cdots (1 - X_vx) = 1 + \Lambda_1x + \Lambda_2x^2 + \cdots + \Lambda_vx^v.
\]

(5)

• Multiplying (5) by \(Y_iX_i^{j+v}\), where \(1 \leq j \leq v\), and set \(x = X_i^{-1}\)
we have

\[ 0 = Y_i X_i^{j+v} \left( 1 + \Lambda_1 X_i^{-1} + \Lambda_2 X_i^{-2} + \cdots + \Lambda_v X_i^{-v} \right). \]

for \( 1 \leq i \leq v \).

- Summing all above \( v \) equations, we have

\[
0 = \sum_{i=1}^{v} Y_i \left( X_i^{j+v} + \Lambda_1 X_i^{j+v-1} + \cdots + \Lambda_v X_i^{j} \right)
\]

\[
= \sum_{i=1}^{v} Y_i X_i^{j+v} + \Lambda_1 \sum_{i=1}^{v} Y_i X_i^{j+v-1} + \cdots + \Lambda_v \sum_{i=1}^{v} Y_i X_i^{j}
\]

\[
= S_{j+v} + \Lambda_1 S_{j+v-1} + \Lambda_2 S_{j+v-2} + \cdots + \Lambda_v S_j.
\]

- We have

\[
\Lambda_1 S_{j+v-1} + \Lambda_2 S_{j+v-2} + \cdots + \Lambda_v S_j = -S_{j+v}
\]

for \( 1 \leq j \leq v \).
• Putting the above equations into matrix form we have

$$\begin{bmatrix}
S_1 & S_2 & \cdots & S_{v-1} & S_v \\
S_2 & S_3 & \cdots & S_v & S_{v+1} \\
\vdots \\
S_v & S_{v+1} & \cdots & S_{2v-2} & S_{2v-1}
\end{bmatrix} \begin{bmatrix}
\Lambda_1 \\
\Lambda_{v-1} \\
\vdots \\
\Lambda_v
\end{bmatrix} = \begin{bmatrix}
-S_{v+1} \\
-S_{v+2} \\
\vdots \\
-S_{2v}
\end{bmatrix}. \quad (6)$$

• Since $v \leq t$, $S_1, S_2, \ldots, S_{2v}$ are all known. Then we can solve for $\Lambda_1, \Lambda_2, \ldots, \Lambda_v$.

• We still need to find the smallest $v$ such that the above system of equations has a unique solution.
Let the matrix of syndromes, $M$, be defined as follows:

$$
M = \begin{bmatrix}
S_1 & S_2 & \cdots & S_u \\
S_2 & S_3 & \cdots & S_{u+1} \\
\vdots & \vdots & \ddots & \vdots \\
S_u & S_{u+1} & \cdots & S_{2u-1}
\end{bmatrix}.
$$

$M$ is nonsingular if $u$ is equal to $v$, the number of errors that actually occurred. $M$ is singular if $u > v$.

**Proof:** Let

$$
A = \begin{bmatrix}
1 & 1 & \cdots & 1 \\
X_1 & X_2 & \cdots & X_u \\
\vdots & \vdots & \ddots & \vdots \\
X_1^{u-1} & X_2^{u-1} & \cdots & X_u^{u-1}
\end{bmatrix}
$$
with $A_{ij} = X_j^{i-1}$ and

$$B = \begin{bmatrix}
Y_1X_1 & 0 & \cdots & 0 \\
0 & Y_2X_2 & \cdots & 0 \\
0 & 0 & \cdots & Y_uX_u
\end{bmatrix}$$

with $B_{ij} = Y_iX_i\delta_{ij}$, where

$$\delta_{ij} = \begin{cases} 
1 & i = j \\
0 & i \neq j
\end{cases}.$$ 

We have

$$(ABAT^T)_{ij} = \sum_{\ell=1}^{u} X_\ell^{i-1} \sum_{k=1}^{u} Y_\ell X_\ell \delta_{\ell k} X_k^{j-1}$$
\[
\begin{align*}
&= \sum_{\ell=1}^{u} X_{\ell}^{i-1} Y_{\ell} X_{\ell} X_{\ell}^{j-1} \\
&= \sum_{\ell=1}^{u} Y_{\ell} X_{\ell}^{i+j-1} = M_{ij}.
\end{align*}
\]

Hence, \( M = AB A^T \). If \( u > v \), then \( \det(B) = 0 \) and then \( \det(M) = \det(A) \det(B) \det(A^T) = 0 \). If \( u = v \), then \( \det(B) \neq 0 \). Since \( A \) is a Vandermonde matrix with \( X_i \neq X_j, i \neq j \), \( \det(A) \neq 0 \). Hence, \( \det(M) \neq 0 \).
The Peterson-Gorenstein-Zierler Algorithm

1. Enter $u(x)$
2. Compute syndromes
   $$S_j = u(\alpha^{j-j_0}) \quad j = 1 \ldots 2t$$
3. Set $v = t$
4. If $\det(M) = 0$ then $v \leftarrow v - 1$
   Otherwise, set $v = t$
5. Find error location
   $$X_i \quad (i = 1 \ldots v)$$
   by finding zeros of $\Lambda(x)$
6. Halt

Special Case:
- $j_0 = 1$
- $\alpha, \alpha^2, \ldots, \alpha^{2t}$
Example

Consider the triple-error-correcting $(15, 5)$ BCH code with $g(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}$. Assume that the received vector is $r(x) = x^2 + x^7$. The operating finite field is $GF(2^4)$. Then the syndromes can be calculated as follows:

\[
S_1 = \alpha^7 + \alpha^2 = \alpha^{12}
\]
\[
S_2 = \alpha^{14} + \alpha^4 = \alpha^9
\]
\[
S_3 = \alpha^{21} + \alpha^6 = 0
\]
\[
S_4 = \alpha^{28} + \alpha^8 = \alpha^3
\]
\[
S_5 = \alpha^{35} + \alpha^{10} = \alpha^0 = 1
\]
\[
S_6 = \alpha^{42} + \alpha^{12} = 0.
\]
Set \( v = 3 \), we have

\[
\det(M) = \begin{vmatrix}
S_1 & S_2 & S_3 \\
S_2 & S_3 & S_4 \\
S_3 & S_4 & S_5 \\
\end{vmatrix}
= \begin{vmatrix}
\alpha^{12} & \alpha^9 & 0 \\
\alpha^9 & 0 & \alpha^3 \\
0 & \alpha^3 & 1 \\
\end{vmatrix} = 0.
\]

Set \( v = 2 \), we have

\[
\det(M) = \begin{vmatrix}
S_1 & S_2 \\
S_2 & S_3 \\
\end{vmatrix}
= \begin{vmatrix}
\alpha^{12} & \alpha^9 \\
\alpha^9 & 0 \\
\end{vmatrix} \neq 0.
\]
We then calculate

\[ M^{-1} = \begin{bmatrix} 0 & \alpha^6 \\ \alpha^6 & \alpha^9 \end{bmatrix}. \]

Hence,

\[ \begin{bmatrix} \Lambda_2 \\ \Lambda_1 \end{bmatrix} = M^{-1} \begin{bmatrix} 0 \\ \alpha^3 \end{bmatrix} = \begin{bmatrix} \alpha^9 \\ \alpha^{12} \end{bmatrix} \]

and

\[ \Lambda(x) = 1 + \alpha^{12} x + \alpha^9 x^2 \]
\[ = (1 + \alpha^2 x) (1 + \alpha^7 x) \]
\[ = \alpha^9 (x - \alpha^8) (x - \alpha^{13}). \]

Since \(1/\alpha^8 = \alpha^7\) and \(1/\alpha^{13} = \alpha^2\), we found the error locations.