Nonbinary BCH Codes and Reed-Solomon Codes
Nonbinary BCH Codes and Reed-Solomon Codes

- In addition to the binary codes, there are nonbinary codes.
- If $p$ is a prime number and $q$ is any power of $p$ ($q=p^m$), there are codes with symbols from the Galois field GF($q$). These codes are called $q$-ary codes.
- An $(n, k)$ linear code with symbols from GF($q$) is a $k$-dimensional subspace of the vector space of all $n$-tuples over GF($q$).
- A $q$-ary $(n, k)$ cyclic code is generated by a polynomial of degree $(n-k)$ with coefficients from GF($q$), which is a factor of $X^n-1$.
- Encoding and decoding of $q$-ary codes are similar to that of binary codes.
- For any choice of positive integers $s$ and $t$, there exists a $q$-ary BCH code of length $n=q^s-1$, which can correct any combinational of $t$ or fewer errors and requires no more than $2st$ parity-check digits.
Let $\alpha$ be a primitive element in the Galois field $\text{GF}(q^s)$. The generator polynomial $g(X)$ of a $t$-error-correcting $q$-ary BCH is the polynomial of lowest degree with coefficients from $\text{GF}(q)$ for which $\alpha, \alpha^2, \ldots, \alpha^{2t}$ are roots. Let $\varphi_i(X)$ be the minimal polynomial of $\alpha^i$. Then

$$g(X) = \text{LCM}\{\varphi_1(X), \varphi_2(X), \ldots, \varphi_{2t}(X)\}$$

The degree of each minimal polynomial is $s$ or less. Therefore, the degree of $g(X)$ is at most $2st$, and hence the number of parity-check digits of the code generated by $g(X)$ is no more than $2st$. For $q=2$, we obtain the binary BCH codes.
Nonbinary BCH Codes and Reed-Solomon Codes

- $t$-error-correcting Reed-Solomon code with symbols from $\text{GF}(q)$:
  - $s=1$, Block length: $n=q-1$, # parity-check digits: $n-k=2t$, Minimum distance: $d_{\text{min}}=2t+1$.

- Reed-Solomon codes with code symbols from $\text{GF}(2^m)$ (i.e., $q=2^m$)
  - Let $\alpha$ be a primitive element in $\text{GF}(2^m)$
  - The generator polynomial of code length $2^m-1$ is $g(x) = (x + \alpha)(x + \alpha^2)\ldots(x + \alpha^{2t}) = g_0 + g_1x + \ldots + g_{2t-1}x^{2t-1} + x^{2t}$
  - $(n,n-2t)$ cyclic code and coefficients of $g(X)$ is from $\text{GF}(2^m)$

- Let Message: $a(X) = a_0 + a_1X + a_2X^2 + \ldots + a_{k-1}X^{k-1}$

- In systematic form, the $2t$ parity-check digits are coefficients of $b(X) = R_{g(x)}\left[X^{2t}a(X)\right] = b_0 + b_1X + \ldots + b_{2t-1}X^{2t-1}$ (Sec 5.3)
Nonbinary BCH Codes and Reed-Solomon Codes

- Encoding circuit of a $q$-ary RS code
Nonbinary BCH Codes and Reed-Solomon Codes

- Decoding of RS code:
  \[ v(x) = v_0 + v_1 x + \ldots + v_{n-1} x^{n-1} \]
  \[ r(x) = r_0 + r_1 x + \ldots + r_{n-1} x^{n-1} \]
  \[ e(x) = r(x) - v(x) = e_0 + e_1 x + \ldots + e_{n-1} x^{n-1} \]
  \[ e_i = r_i - v_i, \quad \in GF(2^m) \]

- Suppose the error pattern \( e(x) \) contains \( v \) errors (nonzero components), then \( e(x) = e_{j_1} x^{j_1} + e_{j_2} x^{j_2} + \ldots + e_{j_v} x^{j_v} \)

To determine \( e(x) \), we need error-locations \( x^{j_i} \)'s and the error values (i.e. \( v \) pairs \( (x^{j_i}, e_{j_i}) \)'s)

- In decoding a RS code, the same three steps used for decoding a binary BCH code are required; in addition, a fourth step involving calculation of error values is required.
Nonbinary BCH Codes and Reed-Solomon Codes

Let $\beta_\ell = \alpha^{j_\ell}$, $\ell = 1, 2, \ldots, v$

$s_1 = r(\alpha) = e_{j_1} \beta_1 + e_{j_2} \beta_2 + \ldots + e_{j_v} \beta_v$

$s_2 = r(\alpha^2) = e_{j_1} \beta_1^2 + \ldots + e_{j_v} \beta_v^2$

\vdots

$s_{2t} = r(\alpha^{2t}) = e_{j_1} \beta_1^{2t} + \ldots + e_{j_v} \beta_v^{2t}$

note: $S_i = R_{(x+\alpha^i)}[r(x)] = b_i$

(i.e. $r(x) = a_i(x)(x+\alpha^i) + b_i$)
Nonbinary BCH Codes and Reed-Solomon Codes

(a) over $GF(2^m)$

(b) in binary form

Division circuit
Nonbinary BCH Codes and Reed-Solomon Codes

- To find $\sigma(x)$: the error-location poly. by Berlekamp’s iterative algorithm
  
  $$\sigma(x) = (1 + \beta_1 x)(1 + \beta_2 x) \cdots (1 + \beta_v x)$$
  
  $$= 1 + \sigma_1 x + \cdots + \sigma_v x^v$$

  Once $\sigma(x)$ is found, we can determine the error values.

  Let
  
  $$z(x) = 1 + (s_1 + \sigma_1)x + (s_2 + \sigma_1 s_1 + \sigma_2)x^2 + \cdots + (s_v + \sigma_1 s_{v-1} + \cdots + \sigma_v)x^v$$

- It can be shown that the error value at location $\beta_l = \alpha^{j_l}$ is given by:
  
  $$e_{j_l} = \frac{Z(\beta_l^{-1})}{\prod_{i=1}^{v} (1 + \beta_i \beta_l^{-1})}$$
Nonbinary BCH Codes and Reed-Solomon Codes

- Ex: Consider a triple-error-correcting Reed-Solomon code with symbols from GF(2^4)
  - The generator polynomial of this code is:
    \[ g(x) = (x + \alpha)(x + \alpha^2)\cdots(x + \alpha^6) \]
    \[ = \alpha^6 + \alpha^9 x + \alpha^6 x^2 + \alpha^4 x^3 + \alpha^{14} x^4 + \alpha^{10} x^5 + x^6 \]
  - (15, 9, 3) RS code, \( n = 15 \). \( n - k = 6 \), \( t = 3 \)

\[ r = (000\alpha^7 00\alpha^3 000000\alpha^4 00) \]

\[ r(x) = \alpha^7 x^3 + \alpha^3 x^6 + \alpha^4 x^{12} \]
Nonbinary BCH Codes and Reed-Solomon Codes

- Step 1. Using table 2.8 below to compute syndrome components:

**TABLE 2.8 THREE REPRESENTATIONS FOR THE ELEMENTS OF GF(2^4) GENERATED BY p(X) = 1 + X + X^4**

<table>
<thead>
<tr>
<th>Power representation</th>
<th>Polynomial representation</th>
<th>4-Tuple representation</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>(0 0 0 0)</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>(1 0 0 0)</td>
</tr>
<tr>
<td>(\alpha)</td>
<td>(\alpha)</td>
<td>(0 1 0 0)</td>
</tr>
<tr>
<td>(\alpha^2)</td>
<td>(\alpha^2)</td>
<td>(0 0 1 0)</td>
</tr>
<tr>
<td>(\alpha^3)</td>
<td>(\alpha + \alpha^2)</td>
<td>(0 0 0 1)</td>
</tr>
<tr>
<td>(\alpha^4)</td>
<td>(\alpha^3)</td>
<td>(1 1 0 0)</td>
</tr>
<tr>
<td>(\alpha^5)</td>
<td>(1 + \alpha)</td>
<td>(0 1 1 0)</td>
</tr>
<tr>
<td>(\alpha^6)</td>
<td>(\alpha^2 + \alpha^3)</td>
<td>(0 0 1 1)</td>
</tr>
<tr>
<td>(\alpha^7)</td>
<td>(1 + \alpha)</td>
<td>(1 1 0 1)</td>
</tr>
<tr>
<td>(\alpha^8)</td>
<td>(1 + \alpha^2)</td>
<td>(1 0 1 0)</td>
</tr>
<tr>
<td>(\alpha^9)</td>
<td>(\alpha + \alpha^3)</td>
<td>(0 1 0 1)</td>
</tr>
<tr>
<td>(\alpha^{10})</td>
<td>(1 + \alpha + \alpha^2)</td>
<td>(1 1 1 0)</td>
</tr>
<tr>
<td>(\alpha^{11})</td>
<td>(\alpha + \alpha^2 + \alpha^3)</td>
<td>(0 1 1 1)</td>
</tr>
<tr>
<td>(\alpha^{12})</td>
<td>(1 + \alpha + \alpha^2 + \alpha^3)</td>
<td>(1 1 1 1)</td>
</tr>
<tr>
<td>(\alpha^{13})</td>
<td>(1 + \alpha^2 + \alpha^3)</td>
<td>(1 0 1 1)</td>
</tr>
<tr>
<td>(\alpha^{14})</td>
<td>(1 + \alpha^3)</td>
<td>(1 0 0 1)</td>
</tr>
</tbody>
</table>
Nonbinary BCH Codes and Reed-Solomon Codes

\[ S_1 = r(\alpha) = \alpha^{10} + \alpha^9 + \alpha = \alpha^{12} \]
\[ S_2 = r(\alpha^2) = \alpha^{13} + 1 + \alpha^{13} = 1 \]
\[ S_3 = r(\alpha^3) = \alpha + \alpha^6 + \alpha^{10} = \alpha^{14} \]
\[ S_4 = r(\alpha^4) = \alpha^4 + \alpha^{12} + \alpha^7 = \alpha^{10} \]
\[ S_5 = r(\alpha^5) = \alpha^7 + \alpha^3 + \alpha^4 = 0 \]
\[ S_6 = r(\alpha^6) = \alpha^{10} + \alpha^9 + \alpha = \alpha^{12} \]

- Step 2. Find \( \sigma(x) = 1 + \alpha^7 x + \alpha^4 x^2 + \alpha^6 x^3 \) by filling out table in next slide.
## Nonbinary BCH Codes and Reed-Solomon Codes

<table>
<thead>
<tr>
<th>$\mu$</th>
<th>$\sigma(\mu)(X)$</th>
<th>$d_{\mu}$</th>
<th>$l_{\mu}$</th>
<th>$\mu - l_{\mu}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$-1$</td>
<td>$1$</td>
<td>$1$</td>
<td>$0$</td>
<td>$-1$</td>
</tr>
<tr>
<td>$0$</td>
<td>$1$</td>
<td>$\alpha^{12}$</td>
<td>$0$</td>
<td>$0$</td>
</tr>
<tr>
<td>$1$</td>
<td>$1 + \alpha^{12}X$</td>
<td>$\alpha^7$</td>
<td>$1$</td>
<td>$0$ (take $\rho = -1$)</td>
</tr>
<tr>
<td>$2$</td>
<td>$1 + \alpha^3X$</td>
<td>$1$</td>
<td>$1$</td>
<td>$1$ (take $\rho = 0$)</td>
</tr>
<tr>
<td>$3$</td>
<td>$1 + \alpha^3X + \alpha^3X^2$</td>
<td>$\alpha^7$</td>
<td>$2$</td>
<td>$1$ (take $\rho = 0$)</td>
</tr>
<tr>
<td>$4$</td>
<td>$1 + \alpha^4X + \alpha^{12}X^2$</td>
<td>$\alpha^{10}$</td>
<td>$2$</td>
<td>$2$ (take $\rho = 2$)</td>
</tr>
<tr>
<td>$5$</td>
<td>$1 + \alpha^7X + \alpha^4X^2 + \alpha^6X^3$</td>
<td>$0$</td>
<td>$3$</td>
<td>$2$ (take $\rho = 3$)</td>
</tr>
<tr>
<td>$6$</td>
<td>$1 + \alpha^7X + \alpha^4X^2 + \alpha^6X^3$</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>
Nonbinary BCH Codes and Reed-Solomon Codes

- Step 3. By substituting $1, \alpha, \alpha^2, ..., \alpha^{14}$ into $\sigma(x)$
  \[ \Rightarrow \alpha^3, \alpha^9, \alpha^{12} \text{ are roots of } \sigma(x) \]
  \[ \therefore \alpha^{-3} = \alpha^{12}, \alpha^{-9} = \alpha^6, \alpha^{-12} = \alpha^3 \text{ are the error-location numbers of } e(x) \]
  \[ \therefore e(x) = e_3x^3 + e_6x^6 + e_{12}x^{12} \]

- Step 4. From 6.34, find $z(x) = 1 + \alpha^2 x + x^2 + \alpha^6 x^3$
  \[ \therefore e_3 = \frac{z(\alpha^{-3})}{(1 + \alpha^6 \alpha^{-3})(1 + \alpha^{12} \alpha^{-3})} = \alpha^7 \]
  \[ e_6 = \frac{z(\alpha^{-6})}{(1 + \alpha^3 \alpha^{-6})(1 + \alpha^{12} \alpha^{-6})} = \alpha^3 \]
If \( \beta \) is not a primitive element of \( \text{GF}(2^m) \), then the \( 2^m \)-ary code generated by \( g(x) = (x + \beta)(x + \beta^2) \cdots (x + \beta^{2t}) \) is a nonprimitive \( t \)-error-correcting RS code.

The length \( n \) of this code is simply the order of \( \beta \).

Decoding of a nonprimitive Reed-Solomon code is identical to the decoding of a primitive Reed-Solomon code.