ELEC 405
Error Control Coding and Sequences

Decoding BCH Codes

Decoding BCH Codes

- $c(x)$ is the transmitted codeword
- $2t$ consecutive powers of α are its roots

$$c(\alpha^b) = c(\alpha^{b+1}) = \cdots = c(\alpha^{b+2t-1}) = 0$$

- The received word is $r(x) = c(x)+e(x)$
- The error polynomial is

$$e(x) = e_0+e_1x+ \ldots +e_{n-1}x^{n-1}$$

- The syndromes are

$$S_j = r(\alpha^j) = e(\alpha^j) = \sum_{k=0}^{n-1} e_k (\alpha^j)^k, \qquad j = 1, \cdots, 2t$$

Decoding BCH Codes

- Suppose there are v errors in locations

$$i_1, i_2, \cdots, i_v$$

- The syndromes can be expressed in terms of these error locations

$$S_j = \sum_{l=1}^{v} e_{i_l} (\alpha^j)^{i_l} = \sum_{l=1}^{v} (\alpha^{i_l})^j = \sum_{l=1}^{v} X_l^j, \qquad j = 1, \cdots, 2t$$

- The X_l are the error locators
- The $2t$ syndrome equations can be expanded in terms of the v unknown error locations

Power-Sum Symmetric Equations

$$S_1 = X_1 + X_2 + \cdots + X_v$$

$$S_2 = X_1^2 + X_2^2 + \cdots + X_v^2$$

$$S_3 = X_1^3 + X_2^3 + \cdots + X_v^3$$

$$\vdots$$

$$S_{2t} = X_1^{2t} + X_2^{2t} + \cdots + X_v^{2t}$$

- The power-sum symmetric functions are nonlinear equations.
- Any method for solving these equations is a decoding algorithm for BCH codes.
- The solution is not unique. If the actual number of errors is t or fewer, the solution that yields an error pattern with the smallest number of errors is the correct solution.
- Peterson showed that these equations can be transformed into a series of linear equations.

The Error Locator Polynomial

- The error locator polynomial $\Lambda(x)$ has as its roots the inverses of the v error locators $\{X_l\}$

$$\Lambda(x) = \prod_{l=1}^{v}(1 - X_l x) = \Lambda_v x^v + \ldots + \Lambda_1 x + \Lambda_0$$

- The roots of $\Lambda(x)$ are then $X_1^{-1}, X_2^{-1}, \ldots, X_v^{-1}$
- Now express the coefficients of $\Lambda(x)$ in terms of the $\{X_l\}$ to get the elementary symmetric functions of the error locators

$$\Lambda_0 = 1$$

$$\Lambda_1 = \sum_{i=1}^{\nu} X_i = X_1 + X_2 + \cdots + X_{\nu-1} + X_\nu$$

$$\Lambda_2 = \sum_{i<j} X_i X_j = X_1 X_2 + X_1 X_3 + \cdots + X_{\nu-2} X_\nu + X_{\nu-1} X_\nu$$

$$\Lambda_3 = \sum_{i<j<k} X_i X_j X_k = X_1 X_2 X_3 + X_1 X_2 X_4 + \cdots + X_{\nu-2} X_{\nu-1} X_\nu$$

$$\vdots$$

$$\Lambda_\nu = \prod X_i = X_1 X_2 \cdots X_\nu$$

From these sets of equations we get Newton's identities

$$S_1 + \Lambda_1 = 0$$

$$S_2 + \Lambda_1 S_1 + 2\Lambda_2 = 0$$

$$S_3 + \Lambda_1 S_2 + \Lambda_2 S_1 + 3\Lambda_3 = 0$$

$$\vdots$$

$$S_\nu + \Lambda_1 S_{\nu-1} + \cdots + \Lambda_{\nu-1} S_1 + \nu\Lambda_\nu = 0$$

$$S_{\nu+1} + \Lambda_1 S_\nu + \cdots + \Lambda_{\nu-1} S_2 + \Lambda_\nu S_1 = 0$$

$$\vdots$$

$$S_{2t} + \Lambda_1 S_{2t-1} + \cdots + \Lambda_{\nu-1} S_{2t-\nu+1} + \Lambda_\nu S_{2t-\nu} = 0$$

Error Correction Procedure for BCH Codes

1. Compute the syndrome vector $\mathbf{S} = (S_1, S_2, \ldots, S_{2t})$ from the received polynomial $r(x)$
2. Determine the error locator polynomial $\Lambda(x)$ from the syndromes $S_1, S_2, \ldots, S_{2t}$
3. Determine the error locators $X_1, X_2, \ldots, X_v$ by finding the roots of $\Lambda(x)$
4. Correct the errors in $r(x)$

Binary BCH Codes

- In fields of characteristic 2, i.e., GF(2^m)

$$S_{2j} = \sum_{l=1}^{v} X_l^{2j} = \left(\sum_{l=1}^{v} X_l^{j} \right)^2 = S_j^2$$

thus every second equation in Newton's identities is redundant

Newton's Identities for Binary Codes

$$S_1 + \Lambda_1 = 0$$

$$S_3 + \Lambda_1 S_2 + \Lambda_2 S_1 + \Lambda_3 = 0$$

$$S_5 + \Lambda_1 S_4 + \Lambda_2 S_3 + \Lambda_3 S_2 + \Lambda_4 S_1 + \Lambda_5 = 0$$

$$\vdots$$

$$S_{2t-1} + \Lambda_1 S_{2t-2} + \Lambda_2 S_{2t-3} + \cdots + \Lambda_t S_{t-1} = 0$$

Peterson's Direct Solution

$$\mathbf{A}\boldsymbol{\Lambda} = \begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ S_2 & S_1 & 1 & 0 & \cdots & 0 & 0 \\ S_4 & S_3 & S_2 & S_1 & \cdots & 0 & 0 \\ S_6 & S_5 & S_4 & S_3 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ S_{2t-4} & S_{2t-5} & S_{2t-6} & S_{2t-7} & \cdots & S_{t-2} & S_{t-3} \\ S_{2t-2} & S_{2t-3} & S_{2t-4} & S_{2t-5} & \cdots & S_t & S_{t-1} \end{bmatrix} \begin{bmatrix} \Lambda_1 \\ \Lambda_2 \\ \Lambda_3 \\ \Lambda_4 \\ \vdots \\ \Lambda_{t-1} \\ \Lambda_t \end{bmatrix} = \begin{bmatrix} -S_1 \\ -S_3 \\ -S_5 \\ -S_7 \\ \vdots \\ -S_{2t-3} \\ -S_{2t-1} \end{bmatrix}$$

- If **A** is nonsingular, we can solve **AΛ** = **S** using linear algebra
- If there are t-1 or t errors, **A** has a nonzero determinant and a solution for **Λ** can be obtained
- If fewer than t-1 errors have occurred, delete the last two rows and the two rightmost columns of **A** and check again for singularity
- Continue until the remaining matrix is nonsingular

- There are two possibilities when a solution of $\mathbf{A\Lambda} = \mathbf{S}$ leads to an incorrect error locator polynomial
  1. If the received word is within Hamming distance t of an incorrect codeword, $\Lambda(x)$ will correct to that codeword, causing a decoding error
  2. If the received word is **not** within Hamming distance t of an incorrect codeword, $\Lambda(x)$ will not have the correct number of roots, or will have repeated roots, causing a decoding failure

Peterson's Algorithm

1. Compute the syndromes **S** from **r**.
2. Construct the syndrome matrix **A**.
3. Compute the determinant of **A**, if it is nonzero, go to 5.
4. Delete the last two rows and columns of **A** and go to 3.
5. Solve $\mathbf{A\Lambda} = \mathbf{S}$ to get $\Lambda(x)$.
6. Find the roots of $\Lambda(x)$, if there are an incorrect number of roots or repeated roots, declare a decoding failure.
7. Complement the bit positions in **r** indicated by $\Lambda(x)$. If fewer than t errors have been corrected, verify that the resulting codeword satisfies the syndrome equations. If not, declare a decoding failure.

Peterson's Algorithm (Cont.)

- For simple cases, the equations can be solved directly
- Single error correction $\Lambda_1 = S_1$
- Double error correction

$$\Lambda_1 = S_1 \qquad \Lambda_2 = \frac{S_3 + S_1^3}{S_1}$$

- Triple error correction

$$\Lambda_1 = S_1 \qquad \Lambda_2 = \frac{S_1^2 S_3 + S_5}{S_1^3 + S_3} \qquad \Lambda_3 = \left(S_1^3 + S_3\right) + S_1 \Lambda_2$$

Peterson's Algorithm (Cont.)

- Four error correction

$$\Lambda_1 = S_1 \qquad \Lambda_2 = \frac{S_1\left(S_7 + S_1^7\right) + S_3\left(S_1^5 + S_5\right)}{S_3\left(S_1^3 + S_3\right) + S_1\left(S_1^5 + S_5\right)}$$

$$\Lambda_3 = \left(S_1^3 + S_3\right) + S_1\Lambda_2 \qquad \Lambda_4 = \frac{\left(S_1^2 S_3 + S_5\right) + \left(S_1^3 + S_3\right)\Lambda_2}{S_1}$$

Example 9-1

- (31,21,5) 2 error correcting BCH code

  $g(x) = m_1(x)m_3(x) = (x^5+x^2+1)(x^5+x^4+x^3+x^2+1)$

  $= x^{10}+x^9+x^8+x^6+x^5+x^3+1$

  r = (0010000110011000000000000000000)

  r(x) = $x^2+x^7+x^8+x^{11}+x^{12}$

$$S_1 = r(\alpha) = \alpha^7 \qquad S_2 = S_1^2 = \alpha^{14} \qquad S_3 = r(\alpha^3) = \alpha^8$$

$$S_4 = S_1^4 = \alpha^{28}$$

Example 9-1 (Cont.)

- Double error correction

$$\Lambda_1 = S_1 = \alpha^7$$

$$\Lambda_2 = \frac{S_3 + S_1^3}{S_1} = \frac{\alpha^8 + \left(\alpha^7\right)^3}{\alpha^7} = \alpha^{15}$$

- Error locator polynomial

$$\Lambda(x) = 1 + \alpha^7 x + \alpha^{15} x^2$$

$$= (1 + \alpha^5 x)(1 + \alpha^{10} x)$$

- The error locators are $X_1 = \alpha^5$ and $X_2 = \alpha^{10}$

Example 9-1 (Cont.)

r = (001000001100110000000000000000)

e = (000001000010000000000000000000)

c = (001001011011100000000000000000)

check:

$c(x) = x^2 + x^5 + x^7 + x^8 + x^{10} + x^{11} + x^{12}$

$= x^2 g(x)$

Example 9-4 (Direct Solution)

- Triple error correcting BCH code n=31

  $g(x) = m_1(x)m_3(x)\mathrm{m}_5(\mathrm{x}) =$
  $1+x+x^2+x^3+x^5+x^7+x^8+x^9+x^{10}+x^{11}+x^{15}$

  has 6 consecutive roots $\{\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6\}$

  $r(x) = 1+x^9+x^{11}+x^{14}$

$$S_1 = r(\alpha) = 1 \quad S_2 = S_1^2 = 1 \qquad S_3 = r(\alpha^3) = \alpha^{29}$$

$$S_4 = S_1^4 = 1 \qquad S_5 = r(\alpha^5) = \alpha^{23} \quad S_6 = S_3^2 = \alpha^{27}$$

Example 9-4 (Cont.)

$$\Lambda_1 = S_1 = \alpha^7$$

$$\Lambda_2 = \frac{S_1^2 S_3 + S_5}{S_1^3 + S_3} = \alpha^{16} \qquad \Lambda_3 = \left(S_1^3 + S_3\right) + S_1 \Lambda_2 = \alpha^{17}$$

- Error locator polynomial

$$\Lambda(x) = 1 + x + \alpha^{16} x^2 + \alpha^{17} x^3$$

- The roots are α^{12}, α^{15}, α^{18}
- The errors are at locations 31-12=19, 31-15=16, 31-18=13
- $e(x) = x^{13}+x^{16}+x^{19}$
- $c(x) = r(x)+e(x) = 1+x^9+x^{11}+x^{13}+x^{14}+x^{16}+x^{19}$

Example 9-2

- In this example, the number of errors is less than the number of correctable errors

  $g(x) = 1+x+x^2+x^3+x^5+x^7+x^8+x^9+x^{10}+x^{11}+x^{15}$

  has 6 consecutive roots $\{\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6\}$

  $r(x) = x^{10}$

$$S_1 = r(\alpha) = \alpha^{10} \quad S_2 = S_1^2 = \alpha^{20} \quad S_3 = r(\alpha^3) = \alpha^{30}$$

$$S_4 = S_1^4 = \alpha^9 \quad S_5 = r(\alpha^5) = \alpha^{19} \quad S_6 = S_3^2 = \alpha^{29}$$

Example 9-2 (Cont.)

- The matrix **A** is

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 0 \\ \alpha^{20} & \alpha^{10} & 1 \\ \alpha^{9} & \alpha^{30} & \alpha^{20} \end{bmatrix}$$

- row 3 is equal to α^{20}×row 2
- Therefore remove the 2nd and 3rd rows and columns, giving

$$\mathbf{A} = [1]$$

- Thus $\Lambda_1 = S_1 = \alpha^{10}$ giving $X_1 = \alpha^{10}$ and $e(x) = x^{10}$
- $c(x) = r(x) + e(x) = x^{10} + x^{10} = 0$

Example 9-2 (Cont.)

- Using the direct solution

$$\Lambda_1 = S_1 = \alpha^{10}$$

$$\Lambda_2 = \frac{S_1^2 S_3 + S_5}{S_1^3 + S_3} = \frac{\alpha^{20}\alpha^{30} + \alpha^{19}}{\alpha^{30} + \alpha^{30}} = 0$$

$$\Lambda_3 = \left(S_1^3 + S_3\right) + S_1\Lambda_2 = \alpha^{30} + \alpha^{30} = 0$$