Decoding BCH Codes

- Recall

$$c(x) = p(x) + X^{n-k} m(x)$$
$$= p(x) + q(x)g(x) + p(x)$$
$$= q(x)g(x)$$

By design α^j for $1 \le j \le 2t$ is a root of $g(x)$.

So,

$$c(\alpha^j) = q(\alpha^j)g(\alpha^j) = 0 \qquad \text{for } 1 \le j \le 2t$$

- Treat the received message word polynomial as the sum of a valid codeword polynomial and an error polynomial:

$$r(x) = c(x) + e(x) = \sum_{i=0}^{n-1} r_i X^i$$

- Compute $2t$ syndromes S_j:

$$S_j = r(\alpha^j) = e(\alpha^j) = \sum_{i=0}^{n-1} e_i X^i$$

- Suppose there are $v \le t$ errors located at $i_1, i_2, \ldots i_v$. That means,

$$e_i = \begin{cases} 1 & i = i_1, i_2, \ldots i_v = i_\ell \quad \ell = 1, 2, \ldots v \le t \\ 0 & \text{otherwise} \end{cases}$$

$$S_j = e(\alpha^j) = \alpha^{j i_1} + \alpha^{j i_2} + \ldots + \alpha^{j i_v} \qquad j = 1, 2, \ldots 2t$$

Assign,

$$X_\ell = \alpha^{i_\ell} \qquad \ell = 1, 2, \ldots v \le t$$

then

$$S_j = \sum_{\ell=1}^{v} X_\ell^j \qquad j = 1, 2, \ldots 2t$$

Expanding: $$S_1 = X_1 + X_2 + \dots + X_v$$

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

$$\vdots$$

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

Recognize the S_i are power sum symmetric polynomials.

- Next define an error locator polynomial $\Lambda(x)$:

$$\Lambda(x) = (1 + X_1 x)(1 + X_2 x) \dots (1 + X_v x)$$

$$= \sum_{i=0}^{v} \Lambda_i x^i$$

The roots of $\Lambda(x)$ are the reciprocals of the various X_ℓ

$$\Lambda\left(\frac{1}{X_\ell}\right) = 0 \qquad \ell = 1, 2, \dots v$$

Expand the factored form of $\Lambda(x)$:

$$\Lambda_0 = 1$$

$$\Lambda_1 = X_1 + X_2 + \dots + X_v$$

$$\Lambda_2 = \sum_{i < j \leq v} X_i X_j$$

$$\vdots$$

$$\Lambda_v = X_1 X_2 \dots X_v$$

Recognize the Λ_v are elementary symmetric polynomials.

- The Newton identities relate the power sum and elementary symmetric polynomials. Remembering we are working over GF(2):

$$S_1 = \Lambda_1$$
$$S_2 = S_1^2$$
$$S_3 = \Lambda_1 S_2 + \Lambda_2 S_1 + \Lambda_3$$
$$S_4 = S_2^2$$
$$S_5 = \Lambda_1 S_4 + \Lambda_2 S_3 + \Lambda_3 S_2 + \Lambda_4 S_1 + \Lambda_5$$
$$S_6 = S_3^2$$
$$\vdots$$
$$S_{2t-1} = \Lambda_1 S_{2t-2} + \Lambda_2 S_{2t-3} + \Lambda_3 S_{2t-4} + \dots + \Lambda_t S_{t-1}$$

- The odd numbered syndrome equations above form a system of t equations in t unknowns, the Λ_t. In matrix form:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ S_2 & S_1 & 1 & 0 & \cdots & 0 \\ \vdots & & \ddots & & & \vdots \\ S_{2t-2} & S_{2t-3} & S_{2t-4} & S_{2t-5} & \cdots & S_{t-1} \end{bmatrix} \begin{bmatrix} \Lambda_1 \\ \Lambda_2 \\ \Lambda_3 \\ \vdots \\ \Lambda_t \end{bmatrix} = \begin{bmatrix} S_1 \\ S_3 \\ S_5 \\ \vdots \\ S_{2t-1} \end{bmatrix}$$

$$[A]\,\Lambda] = S]$$

- If the determinant of $[A]$ is nonzero, $[A]$ is non-singular, $[A]^{-1}$ exists and $\Lambda]$ can be found:

$$\Lambda] = [A]^{-1} S]$$

Once the Λ_i are known $\Lambda(x)$ can be constructed and its roots found. If these roots are distinct then the number of errors ν is t or $t-1$. Further, these roots are the reciprocals of the X_ℓ defined earlier. This allows the X_ℓ to be determined.

- Recall $\quad X_\ell = \alpha^{i_\ell} \quad \ell = 1, 2, \ldots \nu$

If the X_ℓ are in fact known then the i_ℓ are known as well:

$$i_\ell = \log_\alpha X_\ell$$

where the $\log_\alpha$ function is defined over the finite field.

- The error polynomial $e(x)$ can now be formed from the error locators i_ℓ.

- Finally the estimated received code polynomial is:

$$\hat{c}(x) = r(x) + e(x)$$

- If the determinant of $[A]$ above is zero then the bottom two rows and rightmost two columns of $[A]$ are eliminated and the process above is repeated. Now the number of errors ν is $t-2$ or $t-3$ if the roots of the new $\Lambda(x)$ are distinct.

Peterson's algorithm:

1. Write down Newton's Identities (N.I.) as above.
2. If $\det[A] = 0$, remove 2 rightmost columns and 2 bottom rows.
3. Test and repeat until $\det[A] \neq 0$
4. Invert and solve for the $\{\Lambda_i\}$.
5. Find roots of $\Lambda(x)$.
   - If roots are not distinct or $\Lambda(x)$ does not have roots in the desired field, go to 9
6. Complement bit positions in received vector that correspond to roots of $\Lambda(x)$.
7. If the corrected word does not satisfy all syndromes, go to 9
8. Output corrected word. STOP
9. Declare decoder failure. STOP