uOttawa

L'Université canadienne
Canada's university

ELG 5372 Error Control Coding

Lecture 18: Decoding of Nonbinary BCH and RS Codes

Université d'Ottawa | University of Ottawa

uOttawa.ca

Nonbinary BCH and RS decoding

- The solution of the error locator polynomial requires some extra work and, once found, the error values must be determined.

$$
\begin{aligned}
S_1 &= e_{i_1} X_1 + e_{i_2} X_2 + \ldots + e_{i_v} X_v \\
S_2 &= e_{i_1} X_1^2 + e_{i_2} X_2^2 + \ldots + e_{i_v} X_v^2 \\
&\vdots \\
S_{2t} &= e_{i_1} X_1^{2t} + e_{i_2} X_2^{2t} + \ldots + e_{i_v} X_v^{2t}
\end{aligned}
$$

- These equations are not power-sum symmetric.

Nonbinary BCH and RS decoding 2

- Let $\Lambda(x) = 1+\Lambda_1 x+\ldots+\Lambda_v x^v$ have roots X_l^{-1}, for $l = 1, 2,\ldots, v$.
- Then, $\Lambda(X_l^{-1}) = 0 = 1+\Lambda_1 X_l^{-1}+\ldots+\Lambda_v X_l^{-v}$
- Multiplying by $e_i^j X_l^j$, we get $0= e_{il} X_l^j(1+\Lambda_1 X_l^{-1}+ \ldots +\Lambda_v X_l^{-v}) = e_{il}(X_l^j+\Lambda_1 X_l^{j-1}+\ldots+\Lambda_v X_l^{j-v})$.
- Summing over all l, we get

$$0 = \sum_{l=1}^{v} e_{i_l} (\Lambda_v X_l^{j-v} + \Lambda_{v-1} X_l^{j-v+1} + \ldots + \Lambda_1 X_l^{j-1} + X_l^j)$$

$$0 = \Lambda_v \sum_{l=1}^{v} e_{i_l} X_l^{j-v} + \Lambda_{v-1} \sum_{l=1}^{v} e_{i_l} X_l^{j-v+1} + \ldots + \Lambda_1 \sum_{l=1}^{v} e_{i_l} X_l^{j-1} + \sum_{l=1}^{v} e_{i_l} X_l^j$$

Nonbinary BCH and RS decoding 3

- Therefore

$$0 = \Lambda_v S_{j-v} + \Lambda_{v-1} S_{j-v+1} + \ldots + \Lambda_1 S_{j-1} + S_j. \quad (***)$$

$$S_j = -\sum_{i=1}^{v} \Lambda_i S_{j-i}, \quad j = v+1, v+2, \ldots, 2t \quad (*)$$

- We used the Berlekamp-Massey Algorithm to solve (*) in the binary case. (*) and (***) are identical. Therefore we can use the Berlekamp-Massey algorithm to solve for Λ_i's in (***) as well.

Forney's Algorithm

- Once the error locations are known, we use Forney's algorithm to find the error values.

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

- Now, we know the values of X_l. We can rewrite (****) as

$$\begin{bmatrix} X_1 & X_2 & X_3 & \cdots & X_v \\ X_1^2 & X_2^2 & X_3^2 & \cdots & X_v^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ X_1^{2t} & X_2^{2t} & X_3^{2t} & \cdots & X_v^{2t} \end{bmatrix} \begin{bmatrix} e_{i_1} \\ e_{i_2} \\ \vdots \\ e_{i_v} \end{bmatrix} = \begin{bmatrix} S_1 \\ S_2 \\ \vdots \\ S_{2t} \end{bmatrix}$$

$$\mathbf{Xe} = \mathbf{S}$$

Forney’s Algorithm 2

- Although we can solve for **e** by inverting **X**, **X** is a Vandermonde matrix.
- We can solve Vandermonde systems in a manner that is less computationally complex than matrix inversion.
- This solution is called Forney’s algorithm.

Forney's Algorithm

- Let $S(x)=\sum_{j=0}^{2t-1} S_{j+1}x^{j}=S_1+S_2x+\ldots+S_{2t}x^{2t-1}$
- And let $\Omega(x)=S(x)\Lambda(x)\bmod x^{2t}$
- Then Forney's algorithm states that

$$e_{i_k}=-\Omega(X_k^{-1})/\Lambda'(X_k^{-1})$$

Proof of Forney's Algorithm

$$1-x^{2t} = (1-x)(1+x+x^2+\ldots+x^{2t-1}) = (1-x)\sum_{i=0}^{2t-1} x^i \quad (1)$$

$$\left(1-x^{2t}\right)\bmod x^{2t} = 1, \text{ therefore } \left[(1-x)\sum_{i=0}^{2t-1} x^i\right]\bmod x^{2t} = 1 \quad (2)$$

$$\begin{aligned}
\Omega(x) &= \left(S(x)\Lambda(x)\right)\bmod x^{2t} \\
&= \left(\left(S_1+S_2x+\ldots+S_{2t}x^{2t-1}\right)\left(\prod_{i=1}^{v}(1-X_ix)\right)\right)\bmod x^{2t} \\
&= \left(\sum_{j=0}^{2t-1}\left(\sum_{l=1}^{v} e_{i_l} X_l^{j+1}\right)x^j\left(\prod_{i=1}^{v}(1-X_ix)\right)\right)\bmod x^{2t} \\
&= \left(\sum_{l=1}^{v} e_{i_l} X_l \sum_{j=0}^{2t-1}(X_lx)^j \prod_{i=1}^{v}(1-X_ix)\right)\bmod x^{2t} \qquad (3)
\end{aligned}$$

Proof of Forney’s Algorithm 2

- Equation (3) can be rewritten as:

$$\Omega(x) = \left(\sum_{l=1}^{v} e_{i_l} X_l \underbrace{\left[(1 - X_l x) \sum_{j=0}^{2t-1} (X_l x)^j \right]}_{1-(X_l x)^{2t}} \prod_{\substack{i=1 \\ i \neq l}}^{v} (1 - X_l x) \right) \bmod x^{2t}$$

- $1-(X_l x)^{2t} \bmod x^{2t} = 1$. Therefore:

$$\Omega(x) = \sum_{l=1}^{v} e_{i_l} X_l \prod_{\substack{i=1 \\ i \neq l}}^{v} (1 - X_l x)$$

Proof of Forney's Algorithm 3

$$\Omega(X_k^{-1}) = \sum_{l=1}^{v} e_{i_l} X_l \prod_{\substack{i=1 \\ i \neq l}}^{v} (1 - X_l X_k^{-1}) \qquad (4)$$

Equation (4) always has a zero in the product except when *l* = *k*. Therefore (4) becomes:

$$\Omega(X_k^{-1}) = e_{i_k} X_k \prod_{\substack{i=1 \\ i \neq k}}^{v} (1 - X_l X_k^{-1}) \qquad (5)$$

Proof of Forney's Algorithm 4

$$\Lambda(x) = \prod_{i=1}^{v} (1 - X_i x)$$

$$\Lambda'(x) = -\sum_{l=1}^{v} X_l \prod_{\substack{i=1 \\ i \neq l}}^{v} (1 - X_i x)$$

$$\Lambda'(X_k^{-1}) = -\sum_{l=1}^{v} X_l \prod_{\substack{i=1 \\ i \neq l}}^{v} (1 - X_i X_k^{-1}) = -X_k \prod_{\substack{i=1 \\ i \neq k}}^{v} (1 - X_i X_k^{-1})$$

Proof of Forney’s Algorithm 5

$$-\Omega(X_k^{-1})/\Lambda'(X_k^{-1}) = \frac{-e_{i_k} X_k \prod_{\substack{i=1 \\ i\neq k}}^{v} (1 - X_l X_k^{-1})}{-X_k \prod_{\substack{i=1 \\ i\neq k}}^{v} (1 - X_l X_k^{-1})} = e_{i_k}$$

Example

- Consider a two error correcting RS code of length 7.
- $g(x) = (x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4)$
- This is a (7,3) 8-ary code.
- Suppose r(x) = $\alpha^3 x+\alpha^4 x^3$.
- $S_1 = \alpha^4+1 = \alpha^5$.
- $S_2 = \alpha^5+\alpha^3 = \alpha^2$.
- $S_3 = \alpha^6+\alpha^6 = 0$.
- $S_4 = \alpha^7+\alpha^9 = 1+\alpha^2 = \alpha^6$.

Example: Berlekamp-Massey to find $\Lambda(x)$

$$\Lambda^{(-1)}(x) = 1$$

$$\Lambda^{(0)}(x) = 1, d_0 = 1$$

$$k = 1, S_1 = \alpha^5, d_1 = \alpha^5, \Lambda^{(1)}(x) = \Lambda^{(0)}(x) + d_0^{-1} d_1 x \Lambda^{(-1)}(x) =$$

$$1 + \alpha^5 x$$

$$k = 2, S_2 = \alpha^2, d_2 = \alpha^2 + \alpha^3 = \alpha^5, \Lambda^{(2)}(x) = \Lambda^{(1)}(x) + d_1^{-1} d_2 x \Lambda^{(0)}(x) =$$

$$1 + \alpha^5 x + x = 1 + \alpha^4 x$$

$$k = 3, S_3 = 0, d_3 = \alpha^6, \Lambda^{(3)}(x) = \Lambda^{(2)}(x) + d_2^{-1} d_3 x \Lambda^{(1)}(x) =$$

$$1 + \alpha^4 x + \alpha x(1 + \alpha^5 x) = 1 + \alpha^2 x + \alpha^6 x$$

$$k = 4, S_4 = \alpha^6, d_4 = \alpha^6 + \alpha = \alpha^5, \Lambda^{(4)}(x) = \Lambda^{(3)}(x) + d_3^{-1} d_4 x \Lambda^{(2)}(x) =$$

$$1 + \alpha^4 x + \alpha^6 x(1 + \alpha^4 x) = 1 + x + \alpha^4 x$$

$$\Lambda(x) = 1 + x + \alpha^4 x^2 = (1 + \alpha x)(1 + \alpha^3 x)$$

$$X_1 = \alpha, X_2 = \alpha^3$$

Example: Finding e_{i1} and e_{i2} using the Forney Algorithm

- $S(x) = \alpha^5+\alpha^2x+\alpha^6x^3$.
- And $\Lambda(x) = 1+x+\alpha^4x^2$.
- Thus $\Omega(x) = (\alpha^5 + (\alpha^2+\alpha^5)x + (\alpha^9+\alpha^2)x^2 + (\alpha^6+\alpha^6)x^3 + \alpha^6x^4 + \alpha^3x^5)\text{mod } x^4 = (\alpha^5 + \alpha^3x + \alpha^6x^4 + \alpha^3x^5)\text{mod } x^4 = \alpha^5 + \alpha^3x$.
- Lastly, $\Lambda'(x) = 1$.
- $e_{i1} = \Omega(X_1^{-1}) / \Lambda'(X_1^{-1}) = \alpha^5+\alpha^3\alpha^6 = \alpha^5+\alpha^2 = \alpha^3$.
- $e_{i2} = \Omega(X_2^{-1}) / \Lambda'(X_2^{-1}) = \alpha^5+\alpha^3\alpha^4 = \alpha^5+1 = \alpha^4$.
- Therefore $e(x) = \alpha^3x+\alpha^4x^3$.
- We decode the received word as $c(x) = r(x)+e(x) = 0$.