5.0 BCH and Reed-Solomon Codes

5.1 Introduction

- A. Hocquenghem (1959), “Codes correcteur d’erreurs;”
- Bose and Ray-Chaudhuri (1960), “Error Correcting Binary Group Codes;”
- First general **family** of algebraic codes defined by **structure**.
- Peterson: proved BCH codes cyclic; first general coding text;
- Gorenstein & Zierler extended to fields of size p^m.
- Decoders developed by Peterson, Zierler, Berlekamp, Massey, Retter, Cooper, others.

5.1.1 Attributes

- cyclic code
- wide selection of n, k, d_{min}
- binary (will relax later) symbols
- efficient encoding and decoding algorithms
- algorithmic definition

5.1.2 Definition

- m, t integers;
- p prime;
- $q = p^m$;
- Let α be an element of order n in $GF(q^m)$.

Basic definition of binary BCH codes:

Definition 1 *For* $m \geq 3$ *and* $t < 2^{m-1}$ *there exists a binary BCH code with*

- *block length* $n = 2^m - 1$
- $n - k \leq mt$
- $d_{min} \geq 2t + 1$

$\square$

The generator polynomial $g(x)$ of this code is the *lowest-degree* polynomial over GF(2) which has $\alpha, \alpha^2, \cdots, \alpha^{2t}$ among its roots.

A more formal and complete definition is:

Definition 2 *For any $t > 0$ and any t_0, a BCH code is the cyclic code with blocklength n and generator polynomial*

$$g(x) = LCM\{m_{t_0}(x), m_{t_0+1}(x), \ldots, m_{t_0+2t-1}(x)\}$$

□

where $m_{t_0}(x)$ is the minimal polynomial of $\alpha^{t_0} \in GF(q^m)$.

Definition 3 *A* **primitive** *BCH code is a BCH code for which α is primitive in $GF(q^m)$.* □

5.2 Generating BCH codes

5.2.1 BCH bound and the generator polynomial

Theorem: *If the roots of every codeword $c(x) \in \mathcal{C}$ include $\alpha, \alpha^2, \cdots, \alpha^{2t}$, then the minimum distance of $\mathcal{C}$ is bounded from below by $2t+1$:*

$$d_{min} \geq d_{BCH} = 2t + 1$$

Proof:

$$c(\alpha^j) = 0, \; j = 1, 2, \cdots, 2t$$

$$\sum_{i=0}^{n-1} c_i (\alpha^j)^i = 0, \; j = 1, 2, \cdots, 2t$$

Method of proof: Assume $w_H(\mathbf{c}) = \delta \leq 2t$. Find *contradiction.*

Let

$$\mathbf{H} \triangleq \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & (\alpha^2) & (\alpha^2)^2 & \cdots & (\alpha^2)^{n-1} \\ \vdots & & & & \\ 1 & (\alpha^{2t}) & (\alpha^{2t})^2 & \cdots & (\alpha^{2t})^{n-1} \end{bmatrix}$$

where

$$\mathbf{c} \cdot \mathbf{H}^T = 0$$

Assume:

$$w_H(\mathbf{c}) = \delta \leq 2t$$

Expand $\mathbf{c}\mathbf{H}^T$, keeping only the terms for which $c_j \neq 0$.

$$
\begin{aligned}
\mathbf{0} &= (c_{j_1}, c_{j_2}, \cdots, c_{j_\delta}) \cdot \begin{bmatrix} \alpha^{j_1} & (\alpha^2)^{j_1} & \cdots & (\alpha^{2t})^{j_1} \\ \alpha^{j_2} & (\alpha^2)^{j_2} & \cdots & (\alpha^{2t})^{j_2} \\ \vdots & & & \\ \alpha^{j_\delta} & (\alpha^2)^{j_\delta} & \cdots & (\alpha^{2t})^{j_\delta} \\ & & & \end{bmatrix} \\
&= (c_{j_1}, c_{j_2}, \cdots, c_{j_\delta}) \cdot \begin{bmatrix} \alpha^{j_1} & (\alpha^{j_1})^2 & \cdots & (\alpha^{j_1})^{2t} \\ \alpha^{j_2} & (\alpha^{j_2})^2 & \cdots & (\alpha^{j_2})^{2t} \\ \vdots & & & \\ \alpha^{j_\delta} & (\alpha^{j_\delta})^2 & \cdots & (\alpha^{j_\delta})^{2t} \end{bmatrix} \\
&= (0, 0 \cdots 0)
\end{aligned}
$$

where the last line is a $2t-$tuple of zeros.

- But *each* inner product of $\mathbf{c}$ and a column is individually zero.
- Therefore, the product of $\mathbf{c}$ with any any set of δ columns is a zero vector:

$$\mathbf{0} = (c_{j_1}, c_{j_2}, \cdots, c_{j_\delta}) \cdot \begin{bmatrix} \alpha^{j_1} & (\alpha^{j_1})^2 & \cdots & (\alpha^{j_1})^\delta \\ \alpha^{j_2} & (\alpha^{j_2})^2 & \cdots & (\alpha^{j_2})^\delta \\ \vdots & & & \\ \alpha^{j_\delta} & (\alpha^{j_\delta})^2 & \cdots & (\alpha^{j_\delta})^\delta \end{bmatrix}$$

- Take determinant of the RHS; factor α^{j_i} from the i^{th} row.

$$0 = \alpha^{j_1+j_2+\cdots+j_\delta} \begin{vmatrix} 1 & \alpha^{j_1} & (\alpha^{j_1})^2 & \cdots & (\alpha^{j_1})^{\delta-1} \\ 1 & \alpha^{j_2} & (\alpha^{j_2})^2 & \cdots & (\alpha^{j_2})^{\delta-1} \\ \vdots & & & & \\ 1 & \alpha^{j_\delta} & (\alpha^{j_\delta})^2 & \cdots & (\alpha^{j_\delta})^{\delta-1} \end{vmatrix}$$

- This is a **Van der Monde** determinant and cannot be $= 0$.
- But we assumed that it is 0.
- $\Rightarrow$ contradiction. Therefore $w_H(\mathbf{c}) \geq 2t$. $\square$

5.2.2 BCH code design procedure

Parameters:

- Typically, *communication problem* dictates n and d_{min}.
- k may not be directly specified.

Design methods:

1. For primitive code, if $n \leq 255$, use table in Appendix E of Wicker.
2. For primitive code, if $255 \leq n \leq 1023$, use table in Appendix C of Lin and Costello (1983 and 2004).
3. If you don't have the tables, proceed as follows:

1. Select n and d_{min}.
2. Find α, an n^{th} root of unity. (If α primitive, then so is code.)
3. Select j_0. For convenience, I usually use 0.
4. Need $2t$ consecutive powers of α *and their conjugates* as roots of $g(x)$.
5. Determine all the roots and take LCM to get $g(x)$.
6. Determine G from $g(x)$ if necessary.

5.2.3 Example

Requirement: a 2-error correcting binary code with $n = 15$.

Solution: Use a BCH code. Take:

$$\begin{aligned} 2t &= 4 \\ j_0 &= 0 \ (\mathit{assumed}) \end{aligned}$$

- Find a 15^{th} root α of unity.
  - The smallest field containing an element of order 15 is $GF(16) = GF(2^4)$.
  - Hence, α is *primitive* in $GF(2^4)$.

- Need at least 4 consecutive powers of α as roots of $g(x)$:
  - If α is a root of $g(x)$, then so are $\alpha^2, \alpha^4, \alpha^8$.
  - Still need α^3 as a root.
  - Then $\alpha^6, \alpha^{12}, \alpha^{24} = \alpha^9$ are conjugate roots of α^3.
  - Now, exponents are $1, 2, 3, 4, 6, 8, 9, 12$.
- But only α and α^3 were specified.
- Therefore $m_1(x)$ and $m_3(x)$ divide $g(x)$.

Therefore,

$$g(x) = LCM[m_1(x),\ m_3(x)].$$

- But $m_1(x)$ is of degree 4 and has a primitive root.
- Therefore, $m_1(x)$ is a primitive polynomial.

- One possible $m_1(x)$ is:

$$p(x) = 1 + x + x^4.$$

- Can use $p(\alpha) = 0$ to define arithmetic in $GF(2^4)$.
- Expand $m_3(x)$:

$$\begin{aligned} m_3(x) &= (x-\alpha^3)(x-\alpha^6)(x-\alpha^{12})(x-\alpha^9) \\ &= 1 + x + x^2 + x^3 + x^4 \end{aligned}$$

Finally, $g(x) = LCM[m_1(x),\ m_3(x)] = m_1(x) \cdot m_3(x)$.

$$\begin{aligned} \deg[g(x)] &= n - k = 8 \\ k &= 7 \end{aligned}$$

and the code is a $(15, 7)$ code with $d_{min} \geq 5$.

$$g(x) = 1 + x^4 + x^5 + x^6 + x^7 + x^8$$

5.3 Introduction to Reed-Solomon codes

5.3.1 Code definition and examples

5.3.1.1 The Codes

Definition 4 *A* **Reed-Solomon Code** *is a* q^m-*ary BCH code of length* $n = q^m - 1$.

$\square$

Properties:

- Roots of $g(x)$ include $2t$ consecutive powers of $\alpha \in GF(q^m)$. $\alpha^n = 1$.
- $g(x)$ contains no conjugate roots (*Why?)*
- Therefore, $n - k = 2t = d_{BCH} - 1$ (MDS!)

5.3.1.3 Encoding

1. Jointly select block length n and size q^m of symbol field.

2. Choose error correction capability t.

3. Find a primitive element α in $GF(q^m)$.

4. Form the generator polynomial:

$$g(x) = (x - \alpha) \cdot (x - \alpha^2) \cdots (x - \alpha^{2t})$$

Example:

- $n = 15$
- Symbol field of size 16
- Double error correction

$$\begin{aligned} g(x) &= (x-\alpha)\cdot(x-\alpha^2)(x-\alpha^3)(x-\alpha^4) \\ &= x^4 + \alpha^{13}x^3 + \alpha^6 x^2 + \alpha^3 x + \alpha^{10} \end{aligned}$$

5.3.2 MDS Codes

5.3.2.1 Definition of MDS Codes

Definition 5 *Any LBC which meets the Singleton Bound is called* **Maximum Distance Separable** *(MDS).* □

Theorem: *RS codes are MDS.*

Proof:

$$\begin{aligned} d_{min} &\leq n-k+1 \text{ (Singleton Bound)} \\ d_{min} &\geq 2t+1 = n-k+1 \text{ by construction)} \end{aligned}$$

□

5.3.2.2 Duals

Theorem: *The dual of an MDS code is MDS.*

Proof:

- Assume there is $\mathbf{c}' \in \mathcal{C}^{\perp}$ such that $w_H(\mathbf{c}') < k$.
- This is equivalent to saying $\mathcal{C}^{\perp}$ is non-MDS. *(Why?)*
- Let $c_{w_i} = 0,\ i = 1, 2, \ldots, n-k$ in $\mathcal{C}^{\perp}$.
- Since $\mathbf{H}$ is the generating matrix for $\mathcal{C}^{\perp}$,
  - write the sub-matrix of $\mathbf{H}$ that generates the 0 positions of $\mathbf{c}'$.

$$(0, 0, \cdots, 0)_{n-k} = \sum_{i=1}^{k} a_{w_i} \cdot h_{w_i}$$

or as matrices

$$\mathbf{0} = \mathbf{a}_w \cdot \mathbf{H}_w, \ \ \mathbf{a}_w \neq \mathbf{0}$$

- Therefore, $\mathbf{H}_w$ is $(n-k) \times (n-k)$ *singular* sub-matrix of $\mathbf{H}$.

- **But,** every linear combination of $d-1 = n-k$ columns of $\mathbf{H}$ is linearly independent (property of $\mathcal{C}$).

But this *contradicts* the assumption that $w_H(\mathbf{c}') < k$. $\square$

5.3.2.3 Information sets

Definition 6 *In a linear block code, information set is a set of k codeword coordinates which are linearly independent.*

(Thus, any information set carries k information symbols).

Theorem *Any set of k codeword coordinates of an MDS code is an information set.*

Proof:

- G is a parity check matrix for $\mathcal{C}^{\perp}$.
- $\mathcal{C}^{\perp}$ has $d_{min} = k + 1 \Rightarrow$ any k columns of G are linearly independent.
- Row rank = column rank. Therefore, any $k \times k$ submatrix can be reduced to I_k by elementary row operations.

$\square$

5.3.3 Modified MDS and RS codes

5.3.3.1 Punctured

Theorem: *A punctured (n, k) MDS code is an $(n-1, k)$ MDS code.*

Proof:

- MDS: Any position can be a parity position, therefore punctured.
- Puncturing reduces d_{min} by no more than 1, and
  - $d_{min} \geq (n-1) - k + 1 = n - k$.
  - But, by Singleton bound $d_{min} \leq (n-1) - k + 1$
- Hence, $d_{min} = n - k = (n-1) - k + 1$: MDS. $\square$

5.3.3.2 Shortened

Theorem: *A shortened MDS code is MDS.*

Proof:

- Remove all codewords having 0 in a specified position: $k \to k-1$.
- Delete that position from all codewords: $n \to n-1$.
- In a *subset* of codewords, d_{min} may increase: $d_{min} \geq (n-1)-(k-1)+1 = n-k+1$.
- But by Singleton bound, $d_{min} \leq (n-1)-(k-1)+1$.
- Therefore $d_{min} = (n-1)-(k-1)+1$ and code is MDS. $\square$

5.3.3.3 Extended

Theorem: *A* **narrow sense** $(q-1,k)$ *RS code can be extended, by adding a parity check, to form a noncyclic* (q,k,d) *MDS code.*

Proof: [Due to S. Roman]

- Let $\mathcal{C}$ be a narrow sense $(j_0 = 1)$ $(q-1,k,d)$ RS code.

- Let $c(x) \in \mathcal{C}, \;\; s.t. \; w_H[c(x)] = d.$

- Extend $c(x)$. (Additional parity check on *all* positions.

$$\begin{aligned} \hat{c}(x) &= c(x) + c_n x^n \\ c_n &= -\sum_{i=0}^{n-1} c_i = -c(1) \end{aligned}$$

1. If $c(1) \neq 0$, then $w_H[\hat{c}(x)] = d + 1$.

2. Now, if $c(1) = 0$, then

   - Write $c(x) = p(x)g(x)$
   - Then $c(1) = p(1)g(1) = 0$
   - Since $g(1) \neq 0,\ p(1) = 0$.
   - Therefore $\hat{g}(x) = (x-1)g(x)$ and $\hat{g}(x)|c(x)$.
   - This means that $c(x) \in <\hat{g}(x)>$.
   - Also $\hat{g}(x)$ has $\hat{d} = 2t+1$ zeros.
   - Therefore, $w_H[c(x)] = d+1$: *contradiction!*
   - Since we assumed $w_H[c(x)] = d$, $p(1) \neq 0$ and $c(1) \neq 0$.
   - Therefore $w_H(\hat{c}(x)) = d+1$

$\square$

5.3.3.4 Doubly-extended

Theorem: *Any narrow-sense, singly-extended* $(n+1, k)$ *RS code can be (further) extended to form a noncyclic* $(n+2, k)$ $q-$*ary MDS code by ading the symbol* c_{n+1} *to each code word, such that:*

$$c_{n+1} = -\sum_{j=0}^{n-1} c + j\alpha^{j\delta}$$

where $\delta =$ the BCH bound of the original BCH code. $\square$