5.0 Reed-Solomon Codes and their Relatives

5.1 Summary of the “Conventional” Model of RS Codes

5.1.1 History

- First general **family** of algebraic codes defined by **structure**.
- A. Hocquenghem (1959), “Codes correcteur d’erreurs;”
- Bose and Ray-Chaudhuri (1960), “Error Correcting Binary Group Codes;”
- I.S. Reed and G. Solomon, ”Polynomial codes over certain finite fields,” *Siam J. Ind. and App. Math*, v8, pp 300-304, 1960.
- Decoders developed by Peterson, Zierler, Berlekamp, Massey, Cooper, Retter, Sudan, others.

5.1.2 Definition

Definition 1 *A* **Reed-Solomon Code** *is a cyclic code generated by*

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

where α is primitive in GF(q^m). □

Therefore,

- length $= q^m - 1$
- $d_{min} = 2t + 1$ (will prove using Fourier transforms)
- $n - k = 2t \Rightarrow$ RS codes meet the Singleton Bound

Definition 2 *Any LBC which meets the Singleton Bound is called* **Maximum Distance Separable** *(MDS).* □

Corollary: *RS codes are MDS.* □

5.1.3 Encoding

1. Jointly select size q^m of symbol field and block length $n = q^m - 1$.
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 ($t = 2$)

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

- (15,11) RS code over GF(16), $d_{min} = 5$.

5.1.4 Duals of RS Codes

Theorem 1 *Dual of RS code is an $(n, n-k)$ RS code with $d_{min} = k+1$.* □

Theorem 2 *The dual of an MDS code is MDS.*

Proof: Count the (remaining)roots. □

Dual of previous ex: (15,4) over GF(16), $d_{min} = 12$.

5.1.5 Information sets

Definition 3 *In a linear block code, an information set is a set of k codeword coordinates which are linearly independent.*

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

Theorem 3 *Any set of k codeword coordinates of an MDS code is an information set.* □

5.1.6 Modified MDS and RS codes

5.1.6.1 Punctured

Theorem 4 *A punctured* (n, k) *MDS code is an* $(n-1, k)$ *MDS code.*

Proof: Puncturing does not change information sets. □

5.1.6.2 Shortened

Theorem 5 *A shortened MDS code is MDS.*

Proof:

- To shorten, $k \to k-1$;
- then $n \to n-1$.
- But remaining information sets are not changed.
- $(n-1)-(k-1)=2t$. $\square$

5.1.6.3 Extended

Theorem 6 *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.*

Comments:

- $n \rightarrow n+1$, k unchanged.
- Now, *any* position contains a parity check on the other n.
- Any k positions remain independent

5.1.6.4 Doubly-extended

Theorem 7 *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 adding 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.

Proof:

See text, pp 171-172. □

5.2 Summary of the "Conventional Model" of BCH Codes

5.2.1 Definition

- $t, \ t_0, \ m, \ n$ integers;
- p prime;
- $q = p^m$;
- α of order n in $GF(q^m)$.

Definition 4 *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 5 *A* **primitive** *BCH code is a BCH code for which* α *is primitive in* $GF(q^m)$*.* □

5.2.2 Generating BCH codes

5.2.2.1 BCH bound and the generator polynomial

Theorem 8 *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 $2t + 1$:*

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

We call d_{BCH}

- *BCH (lower) bound* on d_{min}, or
- the *design distance* of the code.

5.2.2.2 To Design a BCH Code

Parameters:

- Select n and d_{min}.
- Determine k by designing the code.
- If k is not satisfactory, REPEAT. ELSE,
  1. Find α, an n^{th} root of unity in some extension field. (If α is primitive, then so is code.)
  2. Select j_0.
  3. Write
  $$g(x) = lcm(m_1(x), m_2(x), \cdots m_{2t}(x))$$
  4. Determine G from $g(x)$ if necessary.

5.2.2.3 Example

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

Solution: Use a BCH code with $2t = 4$ and $d_{BCH} = 5$.

- Let α be a 15^{th} root of unity; take $j_0 = 0$.
  - The smallest field containing an element of order 15 is $GF(16) = GF(2^4)$.
  - Hence, α is *primitive* in $GF(2^4)$.
- Let α be a root of $g(x)$, then so are $\alpha^2, \alpha^4, \alpha^8$.
- Also need α^3 to have 4 consecutive powers.
- So, $g(x) = lcm[m_1(x), m_2(x), m_3(x), m_4(x)]$
- But $m_1(X) = m_2(x) = m_4(x)$ by conjugacy.
- Therefore $g(x) = lcm[m_1(x), m_3(x)] = m_1(x) \cdot m_3(x)$.
- Exponents of roots of $g(x)$ are $\{1, 2, 3, 4, 6, 8, 9, 12\}$.

For example,

$$\begin{aligned}
m_1(x) &= p(x) = 1 + x + x^4 \\
m_3(x) &= (x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^9) \\
&= 1 + x + x^2 + x^3 + x^4 \\
g(x) &= (1 + x + x^4)(1 + x + x^2 + x^3 + x^4) \\
&= 1 + x^4 + x^5 + x^6 + x^7 + x^8 \\
\deg[g(x)] &= n - k = 8 \\
k &= 7.
\end{aligned}$$

So, the code is a $(15, 7)$ code with $d_{min} \geq 5$.
Since $w_H(g(x)) = 5$, $d_{min} = 5$.

5.3 Codes based on the Fourier Transform

5.3.1 Fourier Transforms in Finite Fields

1. Recall Fourier transform:
   - $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$: real or complex.
   - $\mathbf{V} = (V_0, V_1, \ldots, V_{n-1})$: the **discrete Fourier transform** of $\mathbf{v}$, where

$$V_k = \sum_{i=0}^{n-1} e^{j2\pi ik/n} v_i, \;\; k = 0, \ldots, n-1.$$

   - $e^{j2\pi/n}$ is a complex n^{th} root of unity.

2. The Finite Field Fourier Transform (FFFT or GFFT)

- Let $ord(\alpha) = n$ in $GF(q)$.
- Let $\mathbf{v} \in GF(q)^n$.

Definition 6 *The* **Finite Field Fourier Transform** *of* $\mathbf{v}$ *is* $\mathbf{V} = (V_0, V_1, \ldots, V_{n-1})$, *where*

$$V_j = \sum_{i=0}^{n-1} \alpha^{ij} v_i.$$

Then $\mathbf{v}$ and $\mathbf{V}$ are a Fourier transform pair,

$$\mathbf{v} \leftrightarrow \mathbf{V}.$$

- $\mathbf{V}$ has length n because $\alpha^n = 1$.
- $V_j \in GF(q),\ j = 0, 1, \ldots, n-1$.

- DFT exists for every n for real and complex numbers.
- FT exists for $GF(q)$ only if $n|(q-1)$. (Why?)

Now, let

$$n|q^m - 1 \text{ for some } m.$$

Then there exists element ω of order n in $GF(q^m)$ and

$$V_j = \sum_{i=0}^{n-1} \omega^{ij} v_j, \ \mathbf{V} \in GF(q^m)^n.$$

So, in general,

$$\begin{aligned} \mathbf{v} &\in GF(q)^n \\ \mathbf{V} &= \mathcal{F}\{\mathbf{v}\} \\ \mathbf{V} &\in GF(q^m)^n \end{aligned}$$

Note:

- Say $\mathbf{v}$ is *time domain* signal. Then i is a discrete time variable.
- Say $\mathbf{V}$ is *spectrum* of $\mathbf{v}$ or is the *frequency domain* representation, and j is the "frequency."
- Any factor of $q^m - 1$ can be a blocklength of $\mathcal{F}\{\cdot\}$.
- Most interesting is the **primitive** blocklength, $n = q^m - 1$.
- It is easier to decode in the frequency domain (analog to linear systems?).

5.3.2 Properties of the FFFT

Hereafter, let $\{v_i\} \leftrightarrow \{V_j\}$ be a Fourier transform pair.

1. **Additivity**: $\{\lambda v_i + \mu w_i\} \leftrightarrow \{\lambda V_j + \mu W_j\}$ *are a Fourier transform pair.*
   Proof:

$$\begin{aligned}
\mathcal{F}\{\lambda v_i + \mu w_i\} &= \sum \alpha^{ij}(\lambda v_i + \mu w_i) \\
&= \lambda \sum \alpha^{ij} v_i + \mu \sum \alpha^{ij} w_j \\
&= \lambda V_j + \mu W_j
\end{aligned}$$

□

2. **Modulation** $\{v_i \alpha^{il}\} \leftrightarrow \{V_{((j+l))}\}$ *are a Fourier transform pair.*

Proof:

$$\sum_i \alpha^{ij} v_i \alpha^{il} = \sum_i \alpha^{i(j+l)} v_i = V_{j+l}$$

$\square$

3. **Inverses** Over $GF(q)$,

$$v_i = \frac{1}{n}\sum_{j=0}^{n-1} \alpha^{ij} V_j, \; j = 0, 1, \ldots, n-1.$$

Proof: In the Fourier transform, multiply, sum, and re-order.

$$\begin{aligned}
\sum_{j=0}^{n-1} \alpha^{-ij} V_j &= \sum_{j=0}^{n-1} \alpha^{-ij} \sum_{k=0}^{n-1} \alpha^{kj} v_k \\
&= \sum_{k=0}^{n-1} v_k \sum_{j=0}^{n-1} \alpha^{-ij} \alpha^{kj} \\
&= \sum_{k=0}^{n-1} v_k \sum_{j=0}^{n-1} \alpha^{(k-i)j}
\end{aligned}$$

But $q^m - 1 = p^M - 1 = nb$. Therefore, p does not divide n.

Since $\alpha^n = 1$ and

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1), \tag{1}$$

α^{rn} is a root of (1) and

$$\sum_{i=1}^{n-1} \alpha^{ir} = 0$$

if $r \neq 0 \; mod \; n$ and

$$\sum_{i=1}^{n-1} \alpha^{ir} = n = \sum \alpha^{(k-i)j}$$

if $r \equiv 0 \; mod \; n$. □

4. **Convolution** Suppose $e_i = f_i g_i,\ i = 0, \ldots, n-1$. Then, E_j *is the* **cyclic convolution** *of* F_j *and* G_j.

Proof:

$$\begin{aligned} E_j &= \sum_{i=0}^{n-1} \alpha^{ij} f_i g_i \\ &= \frac{1}{n} \sum_{i=0}^{n-1} \alpha^{ij} f_i \sum_{k=0}^{n-1} \alpha^{-ki} G_k \\ &= \frac{1}{n} \sum_{k=0}^{n-1} G_k \left(\sum_{i=0}^{n-1} \alpha^{ij} \alpha^{-ki} f_i \right) \\ &= \frac{1}{n} \sum_{k=0}^{n-1} G_k F_{((j-k))} \end{aligned}$$

where $((\cdot)) \Leftrightarrow\ mod\ n$. This is the formula for cyclic convolution.

Exercise: Show that if $E_i = F_i G_i$ then

$$e_j = \frac{1}{n} \sum_{i=1}^{n-1} f_i g_{((j-i))}.$$

5. **Translation**

$$\begin{aligned} \{v_{((i-l))}\} &\leftrightarrow \{V_j \alpha^{lj}\} \\ \{\alpha^i v_i\} &\leftrightarrow \{V_{((j+1))}\} \\ \{v_{((l-1))}\} &\leftrightarrow \{V_j \alpha^j\} \end{aligned}$$

Proof: Exercise.

6. **Notation**

$$\begin{aligned} v(x) &= v_{n-1}x^{n-1} + \cdots + v_1 x + v_0 \\ V(x) &= V_{n-1}x^{n-1} + \cdots + V_1 x + V_0 \end{aligned}$$

where

$$\{v\} \leftrightarrow \{V\}$$

as before.

Theorem 9 *(a)* $v(\alpha^j) = 0 \Leftrightarrow V_j = 0.$

(b) $V(\alpha^{-j}) = 0 \Leftrightarrow v_j = 0.$

Proof: By direct substitution and observation. □

7. **Decimation**

- $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$.
- Choose b relatively prime to n.
- Let $P : i \rightarrow bi \pmod{n}$ define a permutation $\mathbf{c}'$ of $\mathbf{c}$.

$$\mathbf{c}' \triangleq \mathbf{c}_{((bi))}$$

P is a **cyclic decimation**, choosing every b^{th} component of $\mathbf{c}$ in a cyclic fashion.

Theorem 10 *Let* $GCD(b,n) = 1, bB \equiv 1 \mod n$. *Then,* $\{\mathbf{c}'\} \leftrightarrow \{\mathbf{C}'\}$ *where*

$$C'_j = C_{((Bj))}$$

Proof:

$$GCD(b,n) = 1 \Leftrightarrow bB + nN = 1.$$

So, by definition,

$$\begin{aligned} C'_j &= \sum \alpha^{ij} c'_i \\ &= \sum \alpha^{(bB+nN)ij} c_{((bi))} \\ &= \sum \alpha^{bBij} c_{((bi))} \\ &= \sum \alpha^{i'Bj} c_{i'} \\ &= C_{Bj} \end{aligned}$$

where the last step is by the translation property. □

8. **Linear Complexity** The *Linear Recursion*:

$$V_k = -\sum_{j=1}^{L} A_j V_{k-j}, \; k = L+1, \ldots$$

is characterized by $\mathbf{A} = (A_1, \ldots, A_L)$ and by length L.

Definition 7 $\{\mathbf{A}, L\}$ *is an* **Autoregressive Filter** *that satisfies the recursion.* □

Definition 8 *The length of the shortest linear recursion that generates a sequence* $V_0, V_1, \ldots, V_{n-1}$ *is called the* **linear complexity** *of* $\mathbf{V} = (V_0, V_1, \ldots V_{n-1})$.

Note: Recursion V can be considered as the Fourier transform of an n-tuple. □

Theorem 11 *The linear complexity of a vector* $\mathbf{V}$ *of finite length (cyclically extended?) equals the Hamming weight of its Fourier transform.*

Proof:

For $\mathbf{v} = (v_0, \ldots, v_{n-1})$, let $v_j \neq 0,\ j \in \{i_1, i_2, \ldots, i_d\}$. Consider

$$A(x) = \prod_{l=1}^{d} (1 - x\alpha^{i_l}) = \sum_{k=0}^{d} A_k x^k.$$

Let $a(x)$ be the inverse Fourier transform of $A(x)$. Then,

$$\begin{aligned} a_i &= \frac{1}{n} \sum_{k=0}^{n-1} \alpha^{-ik} A_k = \frac{1}{n} A(\alpha^{-i}) \\ &= \frac{1}{n} \prod_{l=1}^{d} (1 - \alpha^{-i}\alpha^{i}) \end{aligned}$$

Or $a_i = 0 \Leftrightarrow i \in \{i_1, \ldots, i_d\}$. Therefore, $a_i = 0 \Leftrightarrow v_i \neq 0,\ \forall i$, and

$$a_i v_i = 0$$

$\square$

5.3.4 RS Codes by Fourier Transforms

We require:

- Symbols from $GF(q)$ and $n|q-1$.
- Time domain and spectral components from $GF(q)$.

Definition 9 *A* **Reed-Solomon Code** *of length* n *is one for which*

$$C_j = 0,\ j \in \{j_0, j_0+1, j_0+2, \ldots, j_0+2t-1\}.$$

□

From a previous theorem:

$$c(\omega^j) = 0 \Leftrightarrow C_j = 0,\ \text{where } \omega^n = 1.$$

Therefore, if $j_0 = 1$,

$$g(x) = (x-\omega)(x-\omega^2)\cdots(x-\omega^{2t}). \tag{2}$$

Taking the inverse transform produces a *non-systematic code:*

$$c(x) = \mathcal{F}^{-1}\{\mathbf{C}\} = \frac{1}{n}\sum_{i=0}^{n-1} \omega^{-ij} V_i$$

If the order of ω is $q-1$ then ω is primitive and $n = q-1$.
Therefore, for a code satisfying (2), BCH bound requires:

$$d_{min} \geq 2t + 1 = n - k + 1$$

But by Singleton bound:

$$d_{min} \leq 2t + 1 = n - k + 1$$

Therefore, for the RS codes:

$$d_{min} = 2t + 1 = n - k + 1$$

and, for fixed (n, k) no code can have larger d_{min}.

5.3.5 Other Galois Field (Conjugacy) Constraints

In general, for $\{v\} \leftrightarrow \{V\}$

$$v_i \in GF(q), \quad V_j \in GF(q^m)$$

But for arbitrary $V \in \mathbf{F}_{q^m}^n$, in general

$$v \notin \mathbf{F}_q^n$$

which we usually want. (Note similarity to complex $S(f)$ for real $s(t)$.)

Theorem 12 *Let* $V \in \mathbf{F}_{q^m}^n$, $n | q^m - 1$. *Then*

$$v \in \mathbf{F}_q^n \Leftrightarrow V_j^q = V_{((qj))},\ j = 0, 1, \ldots, n-1.$$

Proof of $\Rightarrow$:

For $j = 0, 1, \ldots, n-1$,

$$\begin{aligned} V_j &= \sum_{i=0}^{n-1} \omega^{ij} v_i \\ V_j^q &= \left(\sum_{i=0}^{n-1} \omega^{ij} v_i \right)^q \\ &= \sum_{i=0}^{n-1} \omega^{iqj} v_i^q \\ &= \sum_{i=0}^{n-1} \omega^{iqj} v_j \\ &= V_{((qj))} \end{aligned}$$

Proof of $\Leftarrow$:

Suppose

$$V_j^q = V_{((jq))}.$$

Then,

$$\sum_{i=0}^{n-1} \omega^{iqj} v_i^q = \sum_{i=0}^{n-1} \omega^{iqj} v_i$$

Let $k = qj$. Then,

$$\sum_{i=0}^{n-1} \omega^{ik} v_i^q = \sum_{i=0}^{n-1} \omega^{ik} v_i \;\; j = 0, \ldots, n-1$$

But both sides are F.T.s, and the F.T. is *unique.* Therefore,

$$v_i^q = v_i \Rightarrow v_i \in \mathbf{F}_q.$$

$\square$

5.3.6 Conjugacy Classes modulo n

Let $m_j =$ the smallest integer for which:

$$jq^{m_j} = j \text{ (modulo)} n$$

Recall that q is relatively prime to n. So the sequence

$$q,\ q^2,\ q^3, \ldots$$

must repeat. Therefore, there is a smallest integer m_j such that all of

$$\{j,\ jq,\ jq^2, \ldots,\ jq^{m_j - 1}\} \tag{3}$$

are distinct, while $jq^{m_j} = j$. We say that (3) is the **conjugacy class containing** j, modulo n.

Note: By the previous theorem, if $\mathbf{c} \in \mathbf{F}_q^n$ then $C_j = C_{jq^l},\ l = 0, 1, \ldots, m_j$. This can be used to design codes as we shall see.

5.3.7 Traces and Idempotents

5.3.7.1 The Trace

Definition 10 *The* $q-$*ary trace of* $\beta \in GF(q^m)$ *is:*

$$
\begin{aligned}
Tr(\beta) &\triangleq \sum_{i=0}^{n-1} \beta^{q^i} \\
&= \beta + \beta^q + \beta^{q^2} + \cdots
\end{aligned}
$$

Since $(a+b)^q = a^q + b^q$,

$$[Tr(\beta)]^q = [Tr(\beta)] \in GF(q)$$

Note that $Tr(\beta)$ is just the sum of the elements in the congugacy class of β. **Exercise:** *Prove that all conjugates have the same trace.*

5.3.7.2 Idempotents

In the spectral domain, let A_k be a conjugacy class and consider a spectrum for which:

$$W_j = \begin{cases} 0, & j \in A_k \\ 1, & j \notin A_k \end{cases}$$

Obviously,

$$W_j^q = W_{((jq))}$$

and the time domain polynomial $w(x) \in \mathbf{F}_q[x]$.

Notice that the j^{th} term of $w^2(x)$ is

$$[\sum_{i=1}^{j} w_i w_{j-i}] x^j$$

- So $w^2(x)$ is a convolution, and its spectrum is given by W_j^2.
- $W_j^2 = W_j$.

Therefore,

$$w^2(x) = w(x) \tag{4}$$

Eq (4) defines an **idempotent**.

Definition 11 *If an idempotent $w(x)$ of a cyclic code satisfies*

$$c(x)w(x) = c(x) \bmod (x^n - 1)$$

$w(x)$ is called a **principal idempotent** *of the code.*

5.3.7.3 Further Results on Idempotents

Construction:

- Let $\{A_i\},\ i \in I$ be a set of conjugacy classes.
- Let $W_i = 0$ if $j \in A_i$ for all $i \in I$, and zero elsewhere.
- Then $w(x) = \mathcal{F}^{-1}\{W\}$ is an idempotent.

Definition 12 *A* **primitive idempotent** *is one constructed from a single conjugacy class. In general an idempotent can be generated as the sum of a set of primitive idempotents.* □

Theorem 13 *Every cyclic code has a unique principal idempotent.*

Proof:

$$W_j = \begin{cases} 0, \; g(\omega^j) & = 0 \\ 1, \; g(\omega^j) & \neq 0 \end{cases}$$

This defines a conjugacy class, so $w(x)$ is an idempotent. Now,

$$g(\omega^j) = 0 \Rightarrow w(\omega^j) = 0.$$

Therefore $w(x) \in$ the code. Also, from the construction above,

$$W_j G_j = G_j$$

so that $w(x)g(x) = g(x)$. Finally,

$$\begin{aligned} c(x) & \in & \mathcal{C} \Rightarrow c(x) = a(x)g(x) \\ c(x)w(x) & = & a(x)w(x)g(x) = a(x)g(x) = c(x) \bmod (x^n - 1). \end{aligned}$$

□

5.3.3 Spectral Representations of Cycic Codes

Time domain polynomial codeword representation:

$$c(x) = a(x)g(x) \ \in \mathbf{F}_q[x]$$

Then

$$c_j = \sum_{i=0}^{k-1} a_i g_{((j-i))}$$

which is the j^{th} term of a **cyclic convolution**:

$$\mathbf{c} = \mathbf{a} * \mathbf{g}$$

Therefore, the spectrum is:

$$C_j = A_j G_j. \tag{5}$$

If $A_j, G_j \in GF(q)$ and $C_j \in GF(q^m)$, then $\mathbf{C}$ defined by (5) is a codeword.

Given an *index set,* $\mathcal{J} = \{j_1, \ldots, j_r\}$, and let

$$\mathcal{C} \triangleq \{\mathbf{c} \in \mathbf{F}_q^n : C_j = 0,\ \forall j \in \mathcal{J}\}$$

Note: This defines a cyclic code.

- By Theorem 9, $\alpha^j = 0 \Leftrightarrow C_j = 0$.
- Therefore, the set $\mathcal{J}$ of frequencies corresponds to the **defining set** $\mathcal{A} = \alpha^j,\ j \in \mathcal{J}$.
- So an alternate definition for a **cyclic code** is:

$$\mathcal{C} = \{\mathcal{F}^{-1}\{C(X)\} : C_j = 0,\ \forall j \in J\}$$

5.3.8 Spectral Specification of BCH Codes

5.3.8.1 Introduction

Suppose we have a vector $\mathbf{v} \in \mathbf{F}_q^n$ where $n|q^m - 1$ such that,

$$\begin{aligned} w_H(\mathbf{v}) &\leq d - 1 \\ 0 &= C_j = C_{j+1} = \cdots = C_{j+2t-1} \end{aligned}$$

for some $0 \leq j \leq n - 1$. Can such a vector exist?

Only if it is the all zero vector...

Theorem 14 *Let* $q^m - 1 = nx$*. Then the only vector in* $\mathbf{F}_q^n$ *of weight* $(d-1)$ *or less having* $(d-1)$ *consecutive spectral zeros is* $\mathbf{0}$*.*

Proof:

- Given $w_H(\mathbf{v}) \leq (d-1)$.
- Recall that the linear complexity of $\mathbf{V} = w_H(\mathbf{v})$.
- Therefore, we write the recursion,

$$V_j = \sum_{l=0}^{d-1} A_l V_{((j-l))}.$$

But if $(d-1)$ consecutive spectral components are zero, this recursion guarantees that all subsequent components will be zero. □

Note that the foregoing theorem gives an alternate definition of the **BCH bound**.

Definition 13 *A BCH code is a code over* $GF(q)$ *that satisfies the BCH bound. In general,*

$$\begin{aligned} C_j &\in GF(q^m) \\ c_j &\in GF(q) \end{aligned}$$

□

Generating BCH Codes

Properties of BCH codes:

- General: $C_j \in GF(q^m),\ c_j \in GF(q)$.
- Special case (RS): $C_j,\ c_j \in GF(q)$.

So,

- Specify $2t$ consecutive spectral zeros.
- BCH bound requires that any nonzero word must have weight $\geq 2t+1$.
- **Therefore** $d_{min} \geq 2t+1 \triangleq d$.
- d is called the "design distance" of the code.

Spectral Domain Specification of BCH Codes

- Select $2t$ consecutive spectral zeros.
- By Theorem 12, other components are constrained and not freely chosen; *i.e.*, given C_j,

$$\begin{aligned} C_{((jq))} &= C_j^q \\ C_{((jq^2))} &= C_j^{q^2} \\ &\vdots \\ C_{((jq^{m_j}-1))} &= C_j^{q^{m_j}-1} \end{aligned}$$

  where
  - $A_j = \{j, jq, \ldots, jq^{m_j-1}\}$, the **conjugacy class containing** j
  - m_j = smallest integer such that $jq^{m_j} = j$.

Therefore,

$$C_j^{q^{mj}} = C_{((jq^{m_j}))} = C_j$$

and,

$$C_j^{q^{m_j}-1} = 1$$

Therefore we can select for C_j only those $\beta \in GF(q^m)$ such that

- $ord\{\beta\} \mid q^{m_j} - 1$, or
- $\beta = 0$.

5.3.8.2 BCH Encoding

Encoding $\Rightarrow$ select a value for each of the $q^m - 1$ positions in the word or in its Fourier Transform.

Procedure:

- Divide the $q^m - 1$ integers into conjugacy classes. (Why?)
- Set $2t$ consecutive frequencies to zero.
- The first element of each remaining conjugacy class is **freely** assignable. The others...?

5.3.8.3 Example

- 3-error correcting BCH code over $GF(2^6)$.
- $C_1 = C_2 = C_3 = C_4 = C_5 = C_6 = 0$.
- Each of these is in a conjugacy clas of size 6, so requires 6 bits to specify.
- The remaining components that can be independently specified are $C_0, C_7, C_9, C_{11}, C_{12}, C_{15}, C_{21}, C_{23}, C_{27}, C_{31}$. All belong to $GF(2^6)$.

However:

$$|A_9| = 3$$

Therefore,

$$C_2^3 = C_9 \ (see\ above\ result).$$

Similarly,

$$|A_{27}| = 3, \ \Rightarrow \ C_{27}^{2^3} = C_{27}$$

Therefore $C_9, C_{27} \in GF(2^3)$. Also,

$$\begin{aligned} |A_{21}| &= 2 \Rightarrow C_{21} \in GF(2^2) \\ |A_0| &= 1 \Rightarrow C_0 \in GF(2) \end{aligned}$$

All others $\in GF(2^6)$ but in no subfield thereof.

Hence, to specify each:

$$\begin{array}{ll} C_0 & 1\ bit \\ C_9 & 3\ bits \\ C_{21} & 2\ bits \\ C_{27} & 3\ bits \\ \hline \\ Total & 9\ bits \end{array}$$

and the remaining $C_7, C_{11}, C_{13}, C_{15}, C_{23}, C_{31}$ require 6 bits each to specify. Hence, we can freely choose $6 \times 6 + 9 = 45$ bits of the codeword, producing a $(63, 45, t = 3)$ BCH code.