

## ECE 771

### Lecture 6 – BCH and RS codes: Designer cyclic codes

**Objective:** We will begin with a result from linear algebra regarding Vandermonde matrices. This result is used to prove the BCH distance properties, which will find ways of designing codes with a stated minimum distance

**Reading:**

- Chapter 8.

**Homework:** 4

1. Problem 8.1, 8.9.

Due Thursday, Nov. 13.

## 1 Vandermonde matrices

A Vandermonde matrix is a matrix of the form

$$V = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ x_0 & x_1 & x_2 & \cdots & x_{n-1} \\ x_0^2 & x_1^2 & x_2^2 & \cdots & x_{n-1}^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_0^{n-1} & x_1^{n-1} & x_2^{n-1} & \cdots & x_{n-1}^{n-1} \end{bmatrix}$$

We will determine an expression for the determinant of  $V$ . Recall that determinants are unmodified by row or column operations. We will do column operations, followed by a cofactor expansion:

$$\begin{aligned} \det(V) &= \det \begin{bmatrix} 1 & 1-1 & 1-1 & \cdots & 1-1 \\ x_0 & x_1-x_0 & x_2-x_0 & \cdots & x_{n-1}-x_0 \\ x_0^2 & x_1^2-x_0 & x_2^2-x_0^2 & \cdots & x_{n-1}^2-x_0^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_0^{n-1} & x_1^{n-1}-x_0^{n-1} & x_2^{n-1}-x_0^{n-1} & \cdots & x_{n-1}^{n-1}-x_0^{n-1} \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ x_0^2 & (x_1-x_0)(x_1+x_0) & (x_2-x_0)(x_2+x_0) & \cdots & (x_{n-1}-x_0)(x_{n-1}+x_0) \\ x_0^3 & (x_1^2+x_0x_1+x_0^2)(x_1-x_0) & (x_2^2+x_0x_2+x_0^2)(x_2-x_0) & \cdots & (x_{n-1}^2+x_0x_{n-1}+x_0^2)(x_{n-1}-x_0) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_0^{n-1} & (x_1^{n-2}+x_1^{n-3}x_0+\cdots+x_0^{n-2})(x_1-x_0) & (x_2^{n-2}+x_2^{n-3}x_0+\cdots+x_0^{n-2})(x_2-x_0) & \cdots & (x_{n-1}^{n-2}+x_{n-1}^{n-3}x_0+\cdots+x_0^{n-2})(x_{n-1}-x_0) \end{bmatrix} \\ &= (1) \prod_{k=1}^n (x_k - x_0) \det \begin{bmatrix} 1 & 1 & \cdots & 1 \\ x_1+x_0 & x_2+x_0 & \cdots & x_{n-1}+x_0 \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{n-2}+x_1^{n-3}x_0+\cdots+x_0^{n-2} & x_2^{n-2}+x_2^{n-3}x_0+\cdots+x_0^{n-2} & \cdots & x_{n-1}^{n-2}+x_{n-1}^{n-3}x_0+\cdots+x_0^{n-2} \end{bmatrix} \end{aligned}$$

Now we repeat the process. We end up with the fact that

$$\det(V) = \prod_{0 \leq j < k \leq n-1} (x_k - x_j)$$

We observe that if the  $\{x_j\}$  are distinct, then the determinant is nonzero, and hence  $V$  is invertible.

## 2 BCH Codes

We are now in a position to state the BCH bound.

**Theorem 1** *Let  $C$  be a  $q$ -ary  $(n, k)$  cyclic code with generator polynomial  $g(x)$ . Let  $GF(q^m)$  be the smallest extension field of  $GF(q)$  that contains a primitive  $n$ th root of unity, and let  $\alpha$  be a primitive  $n$ th root of unity in that field.*

*We will define our  $g(x)$  to be a minimal-degree polynomial in  $GF(q)[x]$  such that:*

$$g(\alpha^b) = g(\alpha^{b+1}) = g(\alpha^{b+2}) = \dots = g(\alpha^{b+\delta-2}) = 0.$$

*That is,  $g$  has  $\delta - 1$  consecutive powers of  $\alpha$  as its zeros. Then, the code  $C$  with generator  $g(x)$  has minimum distance  $\geq \delta$ .*

Ponder the implications: we can choose a distance for our code, and find the generator to match it. The parameter  $\delta$  is called the *design distance* for the code. We may in fact exceed it (and often do for BCH, but not for RS.)

**Proof** Let  $\mathbf{c} \in C$ , with corresponding polynomial representation  $c(x)$ . Then

$$c(\alpha^b) = c(\alpha^{b+1}) = \dots = c(\alpha^{b+\delta-2}) = 0.$$

We can write a parity check matrix for the code as

$$H = \begin{bmatrix} 1 & \alpha^b & \alpha^{2b} & \dots & \alpha^{(n-1)b} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \dots & \alpha^{(n-1)(b+1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{b+\delta-3} & \alpha^{2(b+\delta-3)} & \dots & \alpha^{(n-1)(b+\delta-3)} \\ 1 & \alpha^{b+\delta-2} & \alpha^{2(b+\delta-2)} & \dots & \alpha^{(n-1)(b+\delta-2)} \end{bmatrix}$$

That this is a parity check matrix may be verified by the fact that if  $\mathbf{c} = (c_0, c_1, \dots, c_{n-1})$  is a code sequence, then  $\mathbf{s}^T = H\mathbf{c}^T = \mathbf{0}$  by the zeros of the code polynomial.

Now we will use the fact (theorem 4-9):

The minimum distance of a code  $C$  is equal to the minimum nonzero number of columns of  $H$  which are linearly dependent.

We will do a proof by contradiction: Suppose there is a codeword  $\mathbf{c}$  of weight  $w < \delta$ . We will write the nonzero components of  $\mathbf{c}$  as  $(c_{a_1}, c_{a_2}, \dots, c_{a_w})$ . Then since  $H\mathbf{c}^T = 0$ , we have

$$\begin{bmatrix} \alpha^{a_1 b} & \alpha^{a_2 b} & \alpha^{a_3 b} & \dots & \alpha^{a_w b} \\ \alpha^{a_1(b+1)} & \alpha^{a_2(b+1)} & \alpha^{a_3(b+1)} & \dots & \alpha^{a_w(b+1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha^{a_1(b+\delta-3)} & \alpha^{a_2(b+\delta-3)} & \alpha^{a_3(b+\delta-3)} & \dots & \alpha^{a_w(b+\delta-3)} \\ \alpha^{a_1(b+\delta-2)} & \alpha^{a_2(b+\delta-2)} & \alpha^{a_3(b+\delta-2)} & \dots & \alpha^{a_w(b+\delta-2)} \end{bmatrix} \begin{bmatrix} c_{a_1} \\ c_{a_2} \\ \vdots \\ c_{a_{w-1}} \\ c_{a_w} \end{bmatrix} = \mathbf{0}$$

If we take the first  $w$  rows, we get

$$\begin{bmatrix} \alpha^{a_1 b} & \alpha^{a_2 b} & \alpha^{a_3 b} & \dots & \alpha^{a_w b} \\ \alpha^{a_1(b+1)} & \alpha^{a_2(b+1)} & \alpha^{a_3(b+1)} & \dots & \alpha^{a_w(b+1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha^{a_1(b+w-2)} & \alpha^{a_2(b+w-2)} & \alpha^{a_3(b+w-2)} & \dots & \alpha^{a_w(b+w-2)} \\ \alpha^{a_1(b+w-1)} & \alpha^{a_2(b+w-1)} & \alpha^{a_3(b+w-1)} & \dots & \alpha^{a_w(b+w-1)} \end{bmatrix} \begin{bmatrix} c_{a_1} \\ c_{a_2} \\ \vdots \\ c_{a_{w-1}} \\ c_{a_w} \end{bmatrix} = \mathbf{0}$$

which we write as

$$H' \mathbf{d}^T = \mathbf{0}$$

Let  $H'$  be the square  $w \times w$  matrix on the LHS of this equation. Since  $\mathbf{d} \neq \mathbf{0}$ , we must have that  $H'$  is singular, so that  $\det(H') = 0$ . Note that

$$\det(H') = \alpha^{a_1 b + a_2 b + \dots + a_w b} \begin{bmatrix} 1 & 1 & \dots & 1 \\ \alpha^{a_1} & \alpha^{a_2} & \dots & \alpha^{a_w} \\ \vdots & & & \\ \alpha^{a_1(w-2)} & \alpha^{a_2(w-2)} & \dots & \alpha^{a_w(w-2)} \\ \alpha^{a_1(w-1)} & \alpha^{a_2(w-1)} & \dots & \alpha^{a_w(w-1)} \end{bmatrix}$$

But the latter matrix is a Vandermonde matrix: its determinant is zero iff  $\alpha^x = \alpha^y$  for some  $x$  and  $y$ ,  $x \neq y$ . So there is a contradiction. Hence we conclude that a codeword with weight  $w < \delta$  cannot exist.

On the other hand, there are codes of weight  $\delta$ . Since  $H$  is  $\delta - 1 \times n$ , the rank of the matrix cannot exceed  $\delta$ .  $\square$

Here is how we design BCH codes:

1. Pick  $n$  and  $t$  (the code corrects  $t$  errors)
2. Find the field  $GF(q^m)$  s.t. there is a primitive  $n$ th root of unity.
3. Select  $\delta - 1 = 2t$  consecutive powers of  $\alpha$  starting with  $\alpha^b$  (you pick  $b$ )
4. Let  $g(x)$  be the LCM of the minimal polynomials (over  $GF(q)$ ) of the powers of  $\alpha$ .

If  $b = 1$  in the design procedure, the codes are said to be *narrow sense* BCH codes. If  $n = q^m - 1$ , the BCH code is said to be *primitive*.

**Example 1** Let  $n = 31$ , and let  $\alpha$  be a root of the primitive polynomial  $x^5 + x^2 + 1$  in  $GF(2^5)$ .

Let us take  $b = 1$  and  $\delta = 3$  (that is,  $t = 1$ ). Then the roots of the generator are

$$\alpha, \alpha^2.$$

The minimal polynomials of these happen to be the same (they are in the same cyclotomic coset and are conjugates). Let  $M_{(1)}(x)$  be the minimal polynomial of  $\alpha$  and let  $M_{(2)}(x)$  be the minimal polynomial of  $\alpha^2$ .

$$g(x) = LCM(M_{(1)}(x), M_{(2)}(x)) = M_{(1)}(x) = x^5 + x^2 + 1$$

Since  $\deg(g) = 5$ , we have a (31,26) code.  $\square$

**Example 2** Now let  $t = 2$ , so  $\delta = 5$ . We must have

$$\alpha, \alpha^2, \alpha^3, \alpha^4$$

as roots. Note that  $\alpha, \alpha^2, \alpha^4$  are conjugates. Then

$$\begin{aligned} g(x) &= LCM(M_{(1)}(x), M_{(2)}(x), M_{(3)}(x), M_{(4)}(x)) = M_{(1)}(x)M_{(3)}(x) = (x^5 + x^2 + 1)(x^5 + x^4 + x^3 + x^2 + 1) \\ &= x^{10} + x^9 + x^8 + x^6 + x^5 + x^3 + 1 \end{aligned}$$

So we have a (31, 21) two-error correcting code.  $\square$

### 3 Reed-Solomon codes

In constructing the BCH codes, we looked for generator polynomials over  $GF(q)$ , so we dealt with minimal polynomials and the extra baggage they bring in. With RS codes, we always deal in the bigger field:

**Definition 1** A Reed-Solomon code is a  $q^m$ -ary BCH code of length  $q^m - 1$ .  $\square$

In  $GF(q^m)$ , the minimal polynomial for any element  $\beta$  is simply  $(x - \beta)$ . The generator for a RS code is therefore

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

There are no extra roots brought in due to conjugates in the minimal polynomials, so the degree of  $g$  is exactly what is required to get the desired minimal distance.

**Example 3** Let  $n = 7$ . We want to design a double-error correcting RS code. Let  $\alpha$  be a root of the primitive polynomial  $x^3 + x + 1$ . A narrow-sense generator is

$$g(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^3)(x - \alpha^4) = x^4 + \alpha^3 x^3 + x^2 + \alpha x + \alpha^4.$$

Note that the *coefficients of  $g(x)$  are in  $GF(8)$* , the extension field. We have a  $(7, 3)$  RS code. There are  $8^3$  codewords.  $\square$

### 4 Properties of RS codes

The *Singleton bound* for codes is:

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

A code which achieves this bound is said to be a **maximum-distance separable (MDS)** code.

**Theorem 2** An  $(n, k)$  RS code has minimum distance  $n - k + 1$ . Hence, RS codes are MDS.

**Proof** This is simply an observation. By the Singleton bound we have

$$d_{\min} \leq n - k + 1.$$

By the BCH bound we have

$$d_{\min} \geq \delta.$$

For a RS code, the degree of the generator is always  $(n - k) = (\delta - 1)$ , so

$$d_{\min} \leq n - k + 1.$$

$\square$

**Theorem 3** If  $C$  is MDS, then so is its dual  $C^\perp$ .

## 5 GF-FT approach

There are interesting results that can be obtained using Galois field Fourier Transforms (GF-FT) in relation to coding theory. We get a new spectral interpretation of the BCH and RS codes, which in turn can lead to new decoding algorithms.

**Definition 2** Let  $\mathbf{v} = (v_0, v_1, \dots, v_{n-1})$  be a vector over  $GF(q)$  such that  $n|q^m - 1$ . Let  $\alpha \in GF(q^m)$  have order  $n$ . The GF-FT is

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

□

**Theorem 4** In a field  $GF(q)$  with characteristic  $p$ , The inverse GF-FT is

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

**Proof** Note that  $\alpha$  is a root of  $x^n - 1$ , and that we can write

$$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \dots + x + 1)$$

If  $r \not\equiv 0 \pmod{n}$ , then  $\alpha^r$  must be a zero of  $(x^{n-1} + x^{n-2} + \dots + x + 1)$ . We therefore have

$$\sum_{j=0}^{n-1} \alpha^{rj} = 0 \quad r \not\equiv 0$$

When  $r \equiv 0$  we get

$$\sum_{j=0}^{n-1} \alpha^{rj} = \sum_{j=0}^{n-1} 1 \equiv n$$

In the inverse-sum formula we get

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

□

Familiar properties of Fourier transforms apply:

**Theorem 5** If

$$\begin{aligned} \mathbf{a} &\leftrightarrow A \\ \mathbf{b} &\leftrightarrow B \\ \mathbf{c} &\leftrightarrow C \end{aligned}$$

Then

$$C_j = A_j B_j \quad j = 0, 1, \dots, n-1$$

if and only if

$$\mathbf{c} = \mathbf{a} \circledast \mathbf{b}$$

(cyclic convolution) and

$$c_j = a_j b_j \quad j = 0, 1, \dots, n-1$$

if and only if

$$\mathbf{C} = n^{-1} \mathbf{A} \circledast \mathbf{B}$$

**Definition 3** The spectrum of the polynomial (codevector)  $v(x) = v_0 + v_1x + \dots + v_{n-1}x^{n-1}$  is the GFFT of  $\mathbf{v}$ .  $\square$

**Theorem 6**  $\alpha^j$  is a zero of  $v(x)$  if and only if the  $j$ th frequency component of the spectrum of  $v(x)$  equals zero.

$\alpha^{-i}$  is a zero of  $V(x)$  if and only if the  $i$ th time component  $v_i$  of the inverse transform  $\mathbf{v}$  of  $\mathbf{V}$  equals zero.

**Proof**

$$v(\alpha^j) = v_0 + v_1\alpha^j + \dots + v_{n-1}\alpha^{(n-1)j} = \sum_{i=0}^{n-1} v_i\alpha^{ij} = V_j.$$

The second part is similar.  $\square$

Recall the basic idea of a minimal polynomial: a polynomial  $p(x)$  has its coefficients in the base field  $GF(q)$  iff its roots are conjugates of each other. We have a similar result for the GF-FT:

**Theorem 7** Let  $\mathbf{V}$  be a vector of length  $n$  over  $GF(q^m)$ , where  $n|q^m - 1$  and  $GF(q^m)$  has characteristic  $p$ . The inverse transform  $\mathbf{v}$  of  $\mathbf{V}$  contains elements exclusively from the subfield  $GF(q)$  if and only iff

$$V_j^q \pmod{p} \equiv V_{qj} \pmod{n}, \quad j = 0, 1, \dots, n-1.$$

**Proof** Recall that in  $GF(p^t)$ ,

$$(a + b)^{p^r} = a^r + b^r.$$

Also recall that an element  $\beta \in GF(q^m)$  is in the subfield  $GF(q)$  iff  $\beta^q = \beta$ .

Let  $v_i \in GF(q)$ . Then

$$V_j^q = \left( \sum_{i=0}^{n-1} \alpha^{ij} v_i \right)^q = \sum_{i=0}^{n-1} \alpha^{qij} v_i^q = \sum_{i=0}^{n-1} \alpha^{iqj} v_i = V_{qj} \pmod{n}.$$

Conversely, assume  $V_j^q = V_{qj} \pmod{n}$ . From the definition,

$$V_j^q = \left( \sum_{i=0}^{n-1} \alpha^{ij} v_i \right)^q = \sum_{i=0}^{n-1} \alpha^{iqj} v_i^q$$

and

$$V_{qj} \pmod{n} = \sum_{i=0}^{n-1} \alpha^{iqj} v_i,$$

hence

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

Let  $k = qj \pmod{n}$ . Since  $n = q^m - 1$ ,  $q$  and  $n$  must be relatively prime, so that as  $j$  ranges from 0 to  $n - 1$ ,  $k$  takes on all values in the same range, so we conclude the  $v_i = v_i^q$ .  $\square$

We can now look at the spectrum and make observations about code polynomials.

**Example 4** In  $GF(8)$ :

$$\begin{aligned} M_*(x) &= x \\ M_0(x) &= x + 1 \\ M_1(x) &= (x - \alpha)(x - \alpha^2)(x - \alpha^4) = x^3 + x + 1 \\ M_3(x) &= (x - \alpha^3)(x - \alpha^6)(x - \alpha^5) = x^3 + x^2 + 1 \end{aligned}$$

Now let us find the GF-FT of the coefficients of the polynomials:

$$\begin{aligned} M_*(x) : \mathcal{F}(010000) &= \{\alpha^j\} = (1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6) \\ M_0(x) : \mathcal{F}(1100000) &= \{1 + \alpha^j\} = (0, \alpha^3, \alpha^6, \alpha, \alpha^5, \alpha^4, \alpha^2) \\ M_1(x) : \mathcal{F}(1101000) &= \{1 + \alpha^j + \alpha^{3j}\} = (1, 0, 0, \alpha^4, 0, \alpha^2, \alpha) \\ M_3(x) : \mathcal{F}(1011000) &= \{1 + \alpha^{2j} + \alpha^{3j}\} = (1, \alpha^4, \alpha, 0, \alpha^2, 0, 0). \end{aligned}$$

Note that the positions of the zeros in the spectra correspond to the roots of the minimal polynomials.  $\square$

We can now state the BCH bound in terms of spectra:

**Theorem 8** Let  $n|q^m - 1$  for some  $m$ . A  $q$ -ary  $n$ -tuple with weight  $\leq \delta - 1$  that also has  $\delta - 1$  consecutive zeros in its spectrum must be the all-zero vector.

Perhaps the most important concept of the proof is the *error locator* polynomial. These will arise again in the future.

**Proof** Let  $\mathbf{c}$  have weight  $\nu$ , having nonzero coordinates at  $i_1, i_2, \dots, i_\nu$ . Define the locator polynomial  $\Lambda(x)$  whose zeros correspond to the nonzero coordinates of  $\mathbf{c}$ :

$$\Lambda(x) = (1 - xa^{-i_1})(1 - xa^{-i_2}) \cdots (1 - xa^{-i_\nu}) = \Lambda_0 + \Lambda_1 x + \cdots + \Lambda_\nu x^\nu.$$

We regard this polynomial as a polynomial in the frequency domain. The *inverse* transform of  $\Lambda(x)$  (i.e., its coefficient sequence) is a time domain vector  $\boldsymbol{\lambda}$  that has zero coordinates in the exact positions where  $\mathbf{c}$  has nonzero coordinates. Also, at the positions where  $c_i = 0$ , the  $\lambda_i$  are not zero. Thus  $c_i \lambda_i = 0$  for all  $i$ . We must therefore have  $\mathbf{C} * \boldsymbol{\Lambda} = \mathbf{0}$  (the convolution theorem).

Assume  $\mathbf{c}$  has weight  $\leq \delta - 1$ , while  $\mathbf{C}$  has  $\delta - 1$  consecutive zeros. We will show that this leads to a contradiction. We have  $\Lambda_k$  equal to zero for  $k > \delta - 1$ , and we know that  $\Lambda_0 = 1$ . The convolution in the freq. domain gives us

$$\sum_{k=0}^{n-1} \Lambda_k C_{i-k} = 0$$

so

$$C_i = - \sum_{k=1}^{\delta-1} \Lambda_k C_{i-k}$$

But  $\mathbf{C}$  has  $\delta - 1$  consecutive zeros, so that  $\mathbf{C}$  is all zero. □

Based on our transform interpretation, we note that a RS code can be obtained by selecting as codewords all vectors whose transforms have  $2t$  consecutive zeros (in the same places). We can use this to devise a nonsystematic encoder: zero pad the message, then inverse GFFT to encode.