ELEC 405
Error Control Coding and Sequences

Reed-Solomon Codes

Reed-Solomon Codes

- Non-binary BCH codes
- Consider GF(q)   ($q=p^r$, p prime)
- To construct a nonbinary BCH code with symbols from GF(q), we use the same technique as for binary BCH codes.
- Roots of $g(x)$ are in GF(q^m), $n|q^m$-1

  n-$k \le 2mt$ product of at most 2t minimal polynomials of degree m

  $d \ge 2t+1$

- Choose $2t$ consecutive powers of α, an element of order n in GF(q^m).
- For RS codes, m=1 and α is a primitive element in GF(q), then

$$n = q-1$$

$$n-k \le 2t \longrightarrow n-k = 2t$$

$$d \ge 2t+1 \longrightarrow d \ge n-k+1$$

- From the Singleton bound, $d \le n-k+1$

$\longrightarrow d = n-k+1$ and all RS codes meet the Singleton bound so they are $(n,k,n-k+1)$ codes (MDS)

Reed-Solomon Codes – Minimal Polynomials

- Coefficients of $g(x)$ are in GF(q), roots of $g(x)$ are also in GF(q).
- Minimal polynomial of α is x-α. There are no conjugates since $\alpha^q = \alpha$.
- BCH: $g(x) = (x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})\cdots$

  RS: $g(x) = (x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{2t})$
- RS codes are a subclass of BCH codes.
- Example: q = 256, n = q-1 = 255

Example 8-4 t=2 GF(8)

- n = 8-1 = 7 Form GF(8) from x^3+x+1

α^0	1
α^1	α
α^2	α^2
α^3	$\alpha+1$
α^4	$\alpha^2+\alpha$
α^5	$\alpha^2+\alpha+1$
α^6	α^2+1

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

$$\mathbf{H}=\begin{bmatrix} 1\ \alpha\ \alpha^2\alpha^3\alpha^4\alpha^5\alpha^6 \\ 1\alpha^2\alpha^4\alpha^6\alpha\ \alpha^3\alpha^5 \\ 1\alpha^3\alpha^6\alpha^2\alpha^5\alpha\ \alpha^4 \\ 1\alpha^4\alpha^8\alpha^5\alpha^2\alpha^6\alpha^3 \end{bmatrix}$$

- (7,3,5) RS code

Comparison: RS vs Binary BCH

- RS: $n|q^m$-1 $q = 8, m = 1$ (7,3,5)

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

- Binary BCH: $n|q^m$-1 $q = 2, m = 3$ (7,1,7)

$$g(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4)\boxed{(x-\alpha^6)(x-\alpha^5)}$$

- RS code: $8^3 = 512$ codewords
- Each symbol can be represented as 3 bits, a codeword has $n = 7$ symbols = 21 bits and $k = 3$ data symbols = 9 bits.
- The (7,3,5) RS code can be considered as a (21,9) binary code.
- $t = 2$ symbols - since 5 bit errors may cover 3 symbols, corrects any burst error of 4 bits or less.

Example 8-5 t=3 GF(64)

- n = 64-1 = 63
- α a root of the primitive polynomial x^6+x+1

$$g(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4)(x-\alpha^5)(x-\alpha^6)$$
$$= x^6 + \alpha^{59}x^5 + \alpha^{48}x^4 + \alpha^{43}x^3 + \alpha^{55}x^2 + \alpha^{10}x + \alpha^{21}$$

- (63,57,7) RS code
- $64^{57} = 8.96 \times 10^{102}$ codewords
- $64^{63} = 6.16 \times 10^{113}$ vectors
- sphere volume 9.94×10^{9}

Another Example: GF(7)

- RS codes can be constructed over any field
- Consider $q = 7$, $n = 6$
- First find a primitive element in GF(7)

ø(6) = 2 so two primitive elements

$3^1=3 \quad 3^2=2 \quad 3^3=6 \quad 3^4=4 \quad 3^5=5 \quad 3^6=1 \longrightarrow$ 3 is primitive

$g(x) = (x-3^1)(x-3^2)(x-3^3)(x-3^4)$

$\quad = (x-3)(x-2)(x-6)(x-4)$ (6,2,5) RS

$g'(x) = (x-3^2)(x-3^3)(x-3^4)(x-3^5)$

$\quad = (x-2)(x-6)(x-4)(x-5)$ (6,2,5) RS

- One can pick any group of consecutive roots

$g(x) = (x-3^1)(x-3^2)(x-3^3)$

$= (x-3)(x-2)(x-6)$ (6,3,4) RS

$= x^3+3x^2+x+6$

$g'(x) = (x-3^2)(x-3^3)(x-3^4)$

$= (x-2)(x-6)(x-4)$ (6,3,4) RS

$= x^3+2x^2+2x+1 = g^*(x)$ self reciprocal

$g(x) = (x-3^1)(x-3^2)(x-3^3)(x-3^4)(x-3^5)$

$= (x-3)(x-2)(x-6)(x-4)(x-5)$ (6,1,6) RS

$= x^5+x^4+x^3+x^2+x+1 = g^*(x)$ self reciprocal

Decoding RS Codes

1. Compute the syndromes
2. Determine the error locator polynomial $\Lambda(x)$
3. Determine the error magnitudes from $\Lambda'(x)$ and $\Omega(x)$

$$\Omega(x) = [1 + S(x)]\Lambda(x)$$

4. Evaluate the error locations and the error values at those locations.

Properties of RS Codes

- Since RS codes are cyclic codes, they can always be put in systematic form
- The dual code of an RS code is also MDS
  - C (6,2,5) code over GF(7)
  - $C^{\perp}$ (6,4,3) code over GF(7)
- A punctured RS code is MDS

$$(n,k,n\text{-}k+1) \longrightarrow (n\text{-}u,k,n\text{-}k\text{-}u+1) \quad (6,4,3) \longrightarrow (5,4,2)$$

- A shortened RS codes is MDS

$$(n,k,n\text{-}k+1) \longrightarrow (n\text{-}u,k\text{-}u,n\text{-}k+1) \quad (6,4,3) \longrightarrow (5,3,3)$$

Extended RS Codes

- An (n,k) RS code over GF(q) with $n = q$-1 can be extended to a $(q+1,k)$ MDS code
- There is a technique for constructing such codes which are cyclic
- A very few RS codes can be triply extended to obtain an MDS code
  - $k = 3$ or n-$k = 3$ and $q = 2^m$
  - $n = q+2$