# Reed-Solomon Codes

Qi Zhang

Aarhus University School of Engineering

03/03/2014

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

# $q$-ary Linear Block Codes

- Consider a Galois Field GF($q$) with $q$ elements. It is possible to construct codes with symbols from GF($q$).
- Here $q = p_{\text{prime}}^{i}$. e.g., $p_{\text{prime}} = 2$ and $i = 3$, $q = 2^3$.
- Such codes are called $q$-ary codes or non-binary codes.
- The concepts and properties developed for binary codes can be applied to $q$-ary codes with a few modifications.
- Consider the $n$-dimension vector space of defined over GF($q$):

$$\mathbf{v} = (v_0,\ v_1,\ \ldots,\ v_{n-1})$$

with $v_i \in$ GF($q$) for $0 \leq i < n$.

- The vector addition is defined as:

$$(u_0,\ u_1,\ \ldots,\ u_{n-1}) + (v_0,\ v_1,\ \ldots,\ v_{n-1}) = (u_0 + v_0,\ u_1 + v_1,\ \ldots,\ u_{n-1} + v_{n-1})$$

where the addition $u_i + v_i$ is carried out in GF($q$).

- It is similar to the multiplication which is carried out also in GF($q$).

$$(u_0,\ u_1,\ \ldots,\ u_{n-1}) \cdot (v_0,\ v_1,\ \ldots,\ v_{n-1})^T = \sum_{i=0}^{n-1} u_i \cdot v_i$$

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

# $q$-ary Linear Block Codes

- **Definition**: An $C_b(n, k)$ linear block code with symbols from GF($q$) is simply a $k$-dimension subspace of the vector space defined over GF($q$).
- A $q$-ary linear block code has all the structure and properties of binary block codes.
- The encoding and decoding of $q$-ary linear block codes are the same as for binary linear block codes, except that operations and computation followed the rules in GF($q$).

# $q$-ary Cyclic Codes

- A $q$-ary cyclic code $C_{cyc}(n, k)$ is generated by a polynomial of degree $n - k$ over GF(q).
- Namely, the generator polynomial:

$$g(X) = g_0 + g_1 X + g_2 X^2 + \ldots + g_{n-k-1} X^{n-k-1} + X^{n-k}$$

  where $g_0 \neq 0$ and $g_i \in \mathrm{GF}(q)$.
- $g(X)$ is a factor of $X^n + 1$.
- The code polynomial $c(X)$ of degree $n - 1$ or less and it is a multiple of $g(X)$.

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

# Introduction of Reed-Solomon Codes

- The generator polynomial $g(X)$ of a $t$-error correcting binary BCH codes is the minimum-degree polynomial defined over GF(2) and it has roots $\alpha$, $\alpha^2$, ..., $\alpha^{2t}$ from GF($2^m$).
- Let $\phi_i(X)$ the minimal polynomial of $\alpha^i$, then

$$g(X) = LCM\{\phi_1(X), \phi_2(X), \ldots, \phi_{2t}(X)\}$$

- Generalizing binary BCH codes to q-array BCH codes:
  - The generator polynomial of a $t$-error correcting $q$-ary BCH code is the minimum-degree polynomial defined over GF($q$) and it has roots $\alpha$, $\alpha^2$, ..., $\alpha^{2t}$ from GF($q^m$). Let $\alpha$ be a primitive element in GF($q^m$).
  - If let $\phi_i(X)$ be the minimal polynomial of $\alpha^i$, then

$$g(X) = LCM\{\phi_1(X), \phi_2(X), \ldots, \phi_{2t}(X)\}$$

  - Obviously, if $q = 2$, then it is binary BCH code.
  - For $q$-ary BCH code if $m = 1$, it is a special family of $q$-ary BCH code, called Reed-Solomn (RS) codes.

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

# Introduction of Reed-Solomon Codes

- A RS code $C_{RS}(n,k)$ is able to correct $t$ or less errors and is defined over GF($q$).
- Comparison of the parameters of Binary BCH codes, $q$-ary BCH code and RS codes:

| | Binary BCH code | RS code |
|---|---|---|
| Code length | $n = 2^m - 1$ | $n = q - 1$ |
| Number of parity check | $n - k \leq mt$ | $n - k = 2t$ |
| Minimum distance | $d_{min} \geq 2t + 1$ | $d_{min} = 2t + 1$ |
| Error correct capability | $t$ errors | $t$ errors |

- Two important features of RS code:
  - The code length is one less than the size of the code alphabet.
  - The minimum Hamming distance is one greater than the number of parity check symbols.

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

# Generator polynomial of Reed-Solomon codes

- The generator polynomial of $C_{RS}(n,k)$ has roots of $\alpha, \alpha^2, \ldots, \alpha^{2t}$;
- Here $\alpha$ is a primitive element of GF($q$), $\alpha^{q-1} = 1$;
- So the generator polynomial of $C_{RS}(n,k)$ can be expressed as

$$\begin{aligned} g(X) &= (X+\alpha)(X+\alpha^2)\ldots(X+\alpha^{2t}) \\ &= g_0 + g_1 X + g_2 X^2 + \ldots + g_{2t} X^{2t} \end{aligned}$$

- Comparing with the generator polynomial of binary BCH code:
  - In binary BCH code, the coefficients of $g(X)$ are defined over GF(2), in RS code, the coefficients of $g(X)$, $g_i$, belong to GF($q$).
  - The minimal polynomials $\phi_i(X)$ defined over GF($q$) are of the simple form $\phi_i(X) = X + \alpha^i$.

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

# Generator polynomial of RS code

- Generator polynomial comparison of the double error correcting codes binary BCH code $C_{BCH}(15,7)$ and RS code $C_{RS}(15,11)$:
- Both generator polynomials $g(X)$ have roots of $\alpha, \alpha^2, \alpha^3, \alpha^4$.
- Here $\alpha$ is a primitive element of GF($2^4$) generated by $p_i(X) = 1 + X + X^4$.
  - Let $\phi_i(X)$ be the minimal polynomial of $\alpha^i$ over GF(2), the generator polynomial of $C_{BCH}(15,7)$ is

$$\begin{aligned} g(X) &= \phi_1(X)\phi_3(X) \\ &= (X^4 + X + 1)(X^4 + X^3 + X^2 + X + 1) \\ &= \left[(X+\alpha)(X+\alpha^2)(X+\alpha^4)(X+\alpha^8)\right]\left[(X+\alpha^3)(X+\alpha^6)(X+\alpha^9)(X+\alpha^{12})\right] \end{aligned}$$

  - The generator polynomial of $C_{RS}(15,11)$ is

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

- Code rate of $C_{BCH}(15,7)$ is $R = 7/15$,
- Code rate of $C_{RS}(15,11)$ is $R = 11/15$.

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

# Reed-Solomon codes defined over GF($2^m$)

- Among the generic RS codes, in practice, the RS codes with elements defined over GF($2^m$) is often used.
- In such RS code, each element can have a binary representation in the form of a vector with element of GF(2).
- Code polynomial of RS code can be generally expressed as:

$$c(X) = c_0 + c_1 X + \ldots + c_{n-1} X^{n-1}$$

  - As $c(X) = m(X)g(X)$, generator polynomial is a factor of code polynomial;
  - Therefore, the roots of generator polynomial are also the roots of the code polynomial.
  - There is $c(\alpha) = c(\alpha^2) = \ldots = c(\alpha^i) = \ldots = c(\alpha^{2t}) = 0$
- Substituting $\alpha^i$ into the general code polynomial expression, there is

$$c(\alpha^i) = c_0 + c_1\alpha^i + \ldots + c_{n-1}\alpha^{(n-1)i} = 0$$
$$1 \leq i \leq n - k = 2t$$

# Generator polynomial of RS code Example

- **Example 5.2**: Construct the generator polynomial of an RS code $C_{RS}(7,5)$ that operates over the GF($2^3$) generated by primitive polynomial $p_i(X) = 1 + X^2 + X^3$.
- **Solution**:
  1. Construct GF($2^3$) by the primitive polynomial $p_i(X) = 1 + X^2 + X^3$.
  2. Construct the generator polynomial:
     - As $n = 7,\ k = 5,\ 2t = n - k = 2$, so the $g(X)$ can be expressed as

$$g(X) = (X + \alpha)(X + \alpha^2)$$

# Generator polynomial of RS code Example

- GF($2^3$) generated by $p_i(X) = 1 + X^2 + X^3$:

| Exponential form | Polynomial form | Vector form |
|---|---|---|
| $0$ | $0$ | 0 0 0 |
| $1$ | $1$ | 1 0 0 |
| $\alpha$ | $\alpha$ | 0 1 0 |
| $\alpha^2$ | $\alpha^2$ | 0 0 1 |
| $\alpha^3$ | $1+\alpha^2$ | 1 0 1 |
| $\alpha^4$ | $1+\alpha+\alpha^2$ | 1 1 1 |
| $\alpha^5$ | $1+\alpha$ | 1 1 0 |
| $\alpha^6$ | $\alpha+\alpha^2$ | 0 1 1 |

- The generator polynomial

$$\begin{aligned} g(X) &= (X+\alpha)(X+\alpha^2) \\ &= X^2 + (\alpha+\alpha^2)X + \alpha^3 \\ &= X^2 + \alpha^6 X + \alpha^3 \end{aligned}$$

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

# RS codes in systematic form

- As the generated code is a linear and cyclic code, the systematic form of RS can be obtained by the same approach of a normal cyclic code.
- The message polynomial is expressed by

$$m(X) = m_0 + m_1 X + m_2 X^2 + \ldots + m_{k-1} X^{k-1}$$

1. Multiply message polynomial by $X^{n-k}$, obtaining $X^{n-k}m(X)$
2. Divide $X^{n-k}m(X)$ by generator polynomial $g(X)$, obtaining remainder $p(X)$, there is

$$X^{n-k}m(X) = q(X)g(X) + p(X)$$

3. The code polynomial in systematic form is

$$c(X) = p(X) + X^{n-k}m(X)$$

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

# RS codes in systematic form

- **Example 5.3**: Determine the code vector in systematic form for the RS code of the example 5.2, when the source message is (001 101 111 010 011).
- **Solution**:
  1. Look up in the GF($2^3$) table, obtaining the message polynomial:
  $$m(X) = \alpha^2 + \alpha^3 X + \alpha^4 X^2 + \alpha X^3 + \alpha^6 X^4$$
  2. Obtaining $X^{n-k}m(X)$
  $$\begin{aligned} X^{n-k}m(X) &= X^{7-5}m(X) \\ &= \alpha^2 X^2 + \alpha^3 X^3 + \alpha^4 X^4 + \alpha X^5 + \alpha^6 X^6 \end{aligned}$$
  3. Divide $X^{n-k}m(X)$ by $g(X)$, obtaining $p(X) = \alpha^5 X$
  4. $c(X) = p(X) + X^{n-k}m(X) = \alpha^5 X + \alpha^2 X^2 + \alpha^3 X^3 + \alpha^4 X^4 + \alpha X^5 + \alpha^6 X^6$
  5. Using the vector form of each element to represent the code polynomial into code vector:
  $$\begin{aligned} \mathbf{c} &= (c_0, c_1, c_2, c_3, c_4, c_5, c_6) \\ &= (000\ 110\ 001\ 101\ 111\ 010\ 011) \end{aligned}$$

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

# Syndrome Calculation of RS Codes

- As we know, the relation among the received polynomial, code polynomial and error polynomial:

$$r(X) = c(X) + e(X)$$

- Syndrome calculation is same as in BCH code.
- We replace the variable $X$ by the roots of $c(X)$, $\alpha^i$, $i = 1, 2, \ldots, 2t$. So

$$r(\alpha^i) = c(\alpha^i) + e(\alpha^i) = e(\alpha^i)$$

- Assuming there are $\tau$ errors at location $X^{j_1}, X^{j_2}, \ldots, X^{j_\tau}$, we define the error location number as

$$\beta_i = \alpha^{j_i} \quad i = 1, 2, \ldots, \tau$$

- A system of equations is formed:

$$\begin{aligned}
s_1 &= r(\alpha) = e(\alpha) = e_{j_1}\beta_1 + e_{j_2}\beta_2 + \ldots + e_{j_\tau}\beta_\tau \\
s_2 &= r(\alpha^2) = e(\alpha^2) = e_{j_1}\beta_1^2 + e_{j_2}\beta_2^2 + \ldots + e_{j_\tau}\beta_\tau^2 \\
&\vdots \\
s_{2t} &= r(\alpha^{2t}) = e(\alpha^{2t}) = e_{j_1}\beta_1^{2t} + e_{j_2}\beta_2^{2t} + \ldots + e_{j_\tau}\beta_\tau^{2t}
\end{aligned}$$

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

# Syndrome Calculation of RS Codes Example

- For the particular case of $C_{RS}(n, n-2)$,
- It can correct any error pattern of size $t = 1$.
- Syndrome calculation is

$$\begin{aligned} s_1 &= r(\alpha) = e(\alpha) = e_{j_1}\beta_1 = e_{j_1}\alpha^{j_1} \\ s_2 &= r(\alpha^2) = e(\alpha^2) = e_{j_1}\beta_1^2 = e_{j_1}\alpha^{2j_1} \end{aligned}$$

- Hence,

$$\begin{aligned} \alpha^{j_1} &= \frac{s_2}{s_1} \\ e_{j_1} &= \frac{s_1^2}{s_2} \end{aligned}$$

- The system has two equations. It is able to find two unknown which are the *error location* and *error value*.

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

# Syndrome Calculation of RS Codes Example

- **Example 5.4**: For the RS code of example 5.3, assume the received vector is
  $\mathbf{r} = (000\ 110\ 001\ 101\ 111\ 111\ 011) = (0\ \alpha^5\ \alpha^2\ \alpha^3\ \alpha^4\ \alpha^4\ \alpha^6)$.
  Determine the error location and error value of the single error that occurred in the transmission, find the code polynomial.

# Syndrome Calculation of RS Codes Example

- **Solution**:
  1. The received polynomial is
     $r(X) = \alpha^5 X + \alpha^2 X^2 + \alpha^3 X^3 + \alpha^4 X^4 + \alpha^4 X^5 + \alpha^6 X^6$
  2. Replace the variable $X$ by $\alpha, \alpha^2$ in $r(X)$, obtaining the syndrome equations:

$$\begin{aligned} s_1 &= r(\alpha) = \alpha^6 + \alpha^4 + \alpha^6 + \alpha + \alpha^2 + \alpha^5 = \alpha \\ s_2 &= r(\alpha^2) = 1 + \alpha^6 + \alpha^2 + \alpha^5 + 1 + \alpha^4 = \alpha^6 \end{aligned}$$

  3. Calculate the error location and error value:

$$\alpha^{j_1} = \frac{s_2}{s_1} = \frac{\alpha^6}{\alpha} = \alpha^5 \quad e_{j_1} = \frac{s_1^2}{s_2} = \frac{\alpha^2}{\alpha^6} = \alpha^{-4} = \alpha^3$$

  4. Obtain the error polynomial $e(X) = \alpha^3 X^5$.
  5. So the code polynomial is

$$\begin{aligned} c(X) &= e(X) + r(X) \\ &= \alpha^3 X^5 + \alpha^5 X + \alpha^2 X^2 + \alpha^3 X^3 + \alpha^4 X^4 + \alpha^4 X^5 + \alpha^6 X^6 \\ &= \alpha^5 X + \alpha^2 X^2 + \alpha^3 X^3 + \alpha^4 X^4 + \alpha X^5 + \alpha^6 X^6 \end{aligned}$$

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

# Error location and error polynomials

- We have learned error location and error polynomials in binary BCH codes:
  - Error location polynomials:

$$\sigma(X) = (X - \alpha^{-j_1})(X - \alpha^{-j_2}) \dots (X - \alpha^{-j_\tau}) = \prod_{l=1}^{\tau} (X - \alpha^{-j_l})$$

  - Error evaluation polynomials:

$$W(X) = \sum_{l=1}^{\tau} e_{j_l} \prod_{\substack{i=1 \\ i \neq l}}^{\tau} (X - \alpha^{-j_i})$$

  - Error value is equal to

$$e_{j_l} = \frac{W(\alpha^{-j_l})}{\sigma'(\alpha^{-j_l})}$$

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

# Decoding RS codes using the Euclidean algorithm

- Steps of the Euclidean algorithm for RS code $C_{RS}(n, k)$ with error correction capability $t$:
  - Step 1. Calculate syndrome vector components $s_i = r(\alpha^i)$, $1 \leq i \leq n-k$ then construct syndrome polynomial

$$S(X) = \sum_{j=1}^{n-k} s_j X^{j-1}$$

  - Step 2. If $S(X) = 0$, the received vector is considered as the code vector.
  - Step 3. If $S(X) \neq 0$, the algorithm initialization:

$$\begin{array}{cc} i = -1 & \\ r_{-1}(X) = X^{n-k} & r_0(X) = S(X) \\ t_{-1}(X) = 0 & t_0(X) = 1 \end{array}$$

  - Step 4. Interation parameters are determined as below. The interation stops when $deg(r_i(X)) < deg(t_i(X))$

$$\begin{aligned} r_i(X) &= r_{i-2}(X) - q_i(X) r_{i-1}(X) \\ t_i(X) &= t_{i-2}(X) - q_i(X) t_{i-1}(X) \end{aligned}$$

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

# Decoding RS codes using the Euclidean algorithm

- Step 5. Take $t_i(X)$ after interation stops. Find $\lambda$ which makes $\sigma(X)$ a monic polynomial.

$$\sigma(X) = \lambda t_i(X), \quad W(X) = -\lambda r_i(X)$$

- Step 6. Find roots of $\sigma(X)$ by *Chien search*.
- Step 7. Calculate the error values by substituting the roots of $\sigma(X)$ into error value equations:

$$e_{j_h} = \frac{W(\alpha^{-j_h})}{\sigma'(\alpha^{-j_h})}$$

- Step 8. The error polynomial is constructed as

$$e(X) = e_{j_1} X^{j_1} + e_{j_2} X^{j_2} + \ldots + e_{j_\tau} X^{j_\tau}$$

- Step 9. Error correction is verified:
  - If $e(\alpha^i) \neq r(\alpha^i)$ for any $i = 1 \ldots 2t$, then error correction is discarded.
  - If $e(\alpha^i) = r(\alpha^i)$ for any $i = 1 \ldots 2t$, then $c(X) = r(X) + e(X)$.

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

# Decoding RS codes using the Euclidean algorithm Example

- **Example 5.5**: For the RS code $C_{RS}(7,3)$ defined over GF$(2^3)$, generated by the primitive polynomial $p_i(X) = 1 + X^2 + X^3$, and for the received vector $\mathbf{r} = (000\ 000\ 011\ 000\ 111\ 000\ 000)$. Determine the error polynomial and code polynomial by Euclidean algorithm.

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

# Decoding RS codes using the Euclidean algorithm Example

- **Solution**:
  - Step 1. Look up the GF($2^3$) Table 5.1, the received polynomial $r(X) = \alpha^6 X^2 + \alpha^4 X^4$
  - Step 2. Calculate the components of syndrome vector by $s_i = r(\alpha^i)$, $1 \leq i \leq 2t = 4$:

$$\begin{aligned}
s_1 &= r(\alpha) &= \alpha + \alpha &= 0 \\
s_2 &= r(\alpha^2) &= \alpha^3 + \alpha^5 &= \alpha^6 \\
s_3 &= r(\alpha^3) &= \alpha^5 + \alpha^2 &= \alpha^4 \\
s_4 &= r(\alpha^4) &= \alpha^5 + \alpha^2 &= \alpha^4
\end{aligned}$$

    So syndrome polynomial is $S(X) = \alpha^6 X + \alpha^4 X^2 + \alpha^4 X^3$.
  - Step 3. $S(X) \neq 0$, initialize the algorithm:

| $i$ | $r_i = r_{i-2} - q_i r_{i-1}$ | $q_i$ | $t_i = t_{i-2} - q_i t_{i-1}$ |
|---|---|---|---|
| -1 | $X^{n-k} = X^4$ | - | 0 |
| 0 | $S(X) = \alpha^6 X + \alpha^4 X^2 + \alpha^4 X^3$ | - | 1 |

# Decoding RS codes using the Euclidean algorithm Example

- continuing...
  - Step 4. Execute the recursion until $deg(r_i) < deg(t_i)$

| $i$ | $r_i = r_{i-2} - q_i r_{i-1}$ | $q_i$ | $t_i = t_{i-2} - q_i t_{i-1}$ |
|---|---|---|---|
| -1 | $X^{n-k} = X^4$ | - | 0 |
| 0 | $S(X) = \alpha^6 X + \alpha^4 X^2 + \alpha^4 X^3$ | - | 1 |
| 1 | $\alpha^3 X^2 + \alpha^2 X$ | $\alpha^3 X + \alpha^3$ | $\alpha^3 X + \alpha^3$ |
| 2 | $\alpha^4 X$ | $\alpha X + \alpha^5$ | $\alpha^4 X^2 + \alpha^3 X + \alpha^5$ |

  - Step 5. As $t_i(X) = \alpha^4 X^2 + \alpha^3 X + \alpha^5$, $\lambda = \alpha^3$, So

$$\begin{aligned} \sigma(X) &= \lambda t_i(X) &&= X^2 + \alpha^6 X + \alpha \\ W(X) &= -\lambda r_i(X) &&= \alpha^3 \alpha^4 X = X \end{aligned}$$

  - Step 6. Find the roots of $\sigma(X)$ by *Chien search*. There is

$$\alpha^{-j_1} = \alpha^3 = \alpha^{-4} \qquad \alpha^{-j_2} = \alpha^5 = \alpha^{-2}$$
$$j_1 = 4 \qquad j_2 = 2$$

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

# Decoding RS codes using the Euclidean algorithm Example

- Have known $j_1 = 4, \quad j_2 = 2$, continuing...
  - Step 7. Calculate the error values by substituting the roots of $\sigma(X)$ into error value equations:

$$
\begin{aligned}
e_{j_1} &= \frac{W(\alpha^{-j_1})}{\sigma'(\alpha^{-j_1})} = \frac{\alpha^3}{\alpha^6} = \alpha^4 \\
e_{j_2} &= \frac{W(\alpha^{-j_2})}{\sigma'(\alpha^{-j_2})} = \frac{\alpha^5}{\alpha^6} = \alpha^6
\end{aligned}
$$

  - Step 8. The error polynomial is constructed as

$$e(X) = e_{j_1} X^{j_1} + e_{j_2} X^{j_2} = \alpha^4 X^4 + \alpha^6 X^2$$

  - Step 9. Error correction is verified.
    - As $e(\alpha^i) = r(\alpha^i)$ for any $i$, then $c(X) = r(X) + e(X)$.
    - The code vector is a all-zero vector.

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN