Reed-Solomon Codes I

Qi Zhang

Aarhus University School of Engineering

27/02/2014

1 q-ary Linear Block Codes

2 Introduction of Reed-Solomon Codes

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 $q = p^i_{\text{prime}}$. 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 $v_i \in \text{GF}(q)$ for $0 \le i < n$.
- 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).

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

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:

$$g(X) = g_0 + g_1X + g_2X^2 + \ldots + g_{n-k-1}X^{n-k-1} + X^{n-k}$$

  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 α, α^2, ..., α^{2t} from GF(2^m).
- Let $\phi_i(X)$ the minimal polynomial of α^i, then

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

- 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 α, α^2, ..., α^{2t} from GF(q^m). Let α be a primitive element in GF(q^m).
  - If let $\phi_i(X)$ be the minimal polynomial of α^i, then

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

  - 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.

Generator polynomial of Reed-Solomon codes

- The generator polynomial of $C_{RS}(n, k)$ has roots of $\alpha, \alpha^2, \ldots, \alpha^{2t}$;
- Here α 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 α 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 α^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:

$$c(X) = c_0 + c_1X + \ldots + c_{n-1}X^{n-1}$$

  - 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 α^i into the general code polynomial expression, there is

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

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

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 $\mathrm{GF}(2^3)$ generated by primitive polynomial $p_i(X) = 1 + X^2 + X^3$.
- **Solution**:
  1. Construct $\mathrm{GF}(2^3)$ 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
α	α	0 1 0
α^2	α^2	0 0 1
α^3	$1+\alpha^2$	1 0 1
α^4	$1+\alpha+\alpha^2$	1 1 1
α^5	$1+\alpha$	1 1 0
α^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