6. Minimal polynomials over GF(2^m) and BCH codes

Coding Technology

Preparations

Let $q = p^m$ and $n = q - 1$ (p prime, $m \geq 2$). The primitive element of GF(q) is y, so

$$GF(q) = \{0, 1, y, y^2, \dots, y^{n-1}\}.$$

We already know that the roots of the polynomial $x^n - 1$ are all nonzero elements of GF(q), that is,

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

Preparations

Let $q = p^m$ and $n = q - 1$ (p prime, $m \geq 2$). The primitive element of GF(q) is y, so

$$GF(q) = \{0, 1, y, y^2, \dots, y^{n-1}\}.$$

We already know that the roots of the polynomial $x^n - 1$ are all nonzero elements of GF(q), that is,

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

However, $x^n - 1$ can be regarded as a polynomial over GF(p), and can be decomposed as the product of irreducible polynomials over GF(p):

$$x^n - 1 = p_1(x)p_2(x)\dots p_L(x).$$

Preparations

Each $p_\ell(x)$ ($\ell = 1, \ldots, L$) is a polynomial that is irreducible over GF(p), but has roots over GF(q).

We group the elements of GF(q) according to the $p_\ell(x)$'s. These groups are called the conjugate groups.

Example. For GF(8), we have $q = 8, p = 2, m = 3, n = 7$, and

$$x^7 - 1 \; = (x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) =$$

Preparations

Each $p_\ell(x)$ ($\ell = 1, \ldots, L$) is a polynomial that is irreducible over GF(p), but has roots over GF(q).

We group the elements of GF(q) according to the $p_\ell(x)$'s. These groups are called the conjugate groups.

Example. For GF(8), we have $q = 8, p = 2, m = 3, n = 7$, and

$$\begin{aligned} x^7 - 1 &= (x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) = \\ &= (x-1) \cdot \underbrace{(x^3 + x + 1)}_{(x-y)(x-y^2)(x-y^4)} \cdot \underbrace{(x^3 + x^2 + 1)}_{(x-y^3)(x-y^5)(x-y^6)} , \end{aligned}$$

Preparations

Each $p_\ell(x)$ ($\ell = 1, \ldots, L$) is a polynomial that is irreducible over GF(p), but has roots over GF(q).

We group the elements of GF(q) according to the $p_\ell(x)$'s. These groups are called the conjugate groups.

Example. For GF(8), we have $q = 8, p = 2, m = 3, n = 7$, and

$$\begin{aligned} x^7 - 1 &= (x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) = \\ &= (x-1) \cdot \underbrace{(x^3 + x + 1)}_{(x-y)(x-y^2)(x-y^4)} \cdot \underbrace{(x^3 + x^2 + 1)}_{(x-y^3)(x-y^5)(x-y^6)}, \end{aligned}$$

So the conjugate groups and corresponding minimal polynomials of GF(8) are

$$\begin{aligned} \{1\} &\to x - 1 \\ \{y, y^2, y^4\} &\to x^3 + x + 1 \\ \{y^3, y^5, y^6\} &\to x^3 + x^2 + 1 \end{aligned}$$

BCH codes

A linear cyclic code is called a BCH code over GF(q) if its generator polynomial $g(x)$ has roots $y^1, y^2, \ldots, y^{2t}$. The code can correct t errors.

Remarks.

- $n = q - 1$ for every BCH code.
- The value of k is not specified, and will depend on t.
- $g(x)$ may have additional roots apart from $y^1, y^2, \ldots, y^{2t}$.
- The roots of $g(x)$ contain entire conjugate groups; $g(x)$ is the product of the corresponding minimal polynomials.

Problem 1

(a) Determine the conjugate roots over GF(4).

(b) Determine the corresponding minimal polynomials.

(c) Determine the generator polynomial of the BCH code correcting every single error.

(d) Depict the corresponding shift register architecture and indicate the coefficients.

(The power table over GF(4): $y^0 = 1, y^1 = y, y^2 = y + 1, y^3 = 1.$)

Problem 1

(a) Determine the conjugate roots over GF(4).
(b) Determine the corresponding minimal polynomials.
(c) Determine the generator polynomial of the BCH code correcting every single error.
(d) Depict the corresponding shift register architecture and indicate the coefficients.

(The power table over GF(4): $y^0 = 1, y^1 = y, y^2 = y + 1, y^3 = 1$.)

Solution.

(a)

$$x^3 - 1 = (x - 1)(x^2 + x + 1) = (x - 1)(x - y)(x - y^2),$$

so the conjugate roots are y, y^2.

Problem 1

(a) Determine the conjugate roots over GF(4).

(b) Determine the corresponding minimal polynomials.

(c) Determine the generator polynomial of the BCH code correcting every single error.

(d) Depict the corresponding shift register architecture and indicate the coefficients.

(The power table over GF(4): $y^0 = 1, y^1 = y, y^2 = y + 1, y^3 = 1$.)

Solution.

(a)

$$x^3 - 1 = (x - 1)(x^2 + x + 1) = (x - 1)(x - y)(x - y^2),$$

so the conjugate roots are y, y^2.

(b) $\Phi(x) = (x - y)(x - y^2) = x^2 + x + 1.$

Problem 1

(a) Determine the conjugate roots over GF(4).

(b) Determine the corresponding minimal polynomials.

(c) Determine the generator polynomial of the BCH code correcting every single error.

(d) Depict the corresponding shift register architecture and indicate the coefficients.

(The power table over GF(4): $y^0 = 1, y^1 = y, y^2 = y + 1, y^3 = 1$.)

Solution.

(a)

$$x^3 - 1 = (x - 1)(x^2 + x + 1) = (x - 1)(x - y)(x - y^2),$$

so the conjugate roots are y, y^2.

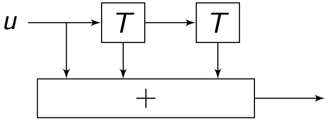
(b) $\Phi(x) = (x - y)(x - y^2) = x^2 + x + 1$.

(c) y and y^2 need to be included among the roots of $g(x)$. They belong to the same conjugate group, so $g(x) = (x - y)(x - y^2) = x^2 + x + 1$.

Problem 1

Solution.

(d)



Side note: each multiplier is implemented by a galvanic connection (due to the nature of minimal polynomials). Thus in GF(2^m), there is no need for complicated "sub shift register" architecture implementing the multiplications.

Problem 2

Can the following polynomial be the generator polynomial of a BCH code over GF(8)?

$$g(x) = x^4 + yx^3 + y^3x^2 + yx + 1$$

Problem 2

Can the following polynomial be the generator polynomial of a BCH code over GF(8)?

$$g(x) = x^4 + yx^3 + y^3x^2 + yx + 1$$

Solution. No, because the generator polynomial of a BCH code over GF(8) must have coefficients from GF(2), so each coefficient must be either 0 or 1.

Problem 3

Give the generator polynomial of the BCH code over GF(8) that can correct 1 error.

Problem 3

Give the generator polynomial of the BCH code over GF(8) that can correct 1 error.

Solution. The conjugate groups and corresponding minimal polynomials of GF(8) are

$$\{1\} \to x - 1$$
$$\{y, y^2, y^4\} \to x^3 + x + 1$$
$$\{y^3, y^5, y^6\} \to x^3 + x^2 + 1$$

To correct $t = 1$ error, $g(x)$ must have y and y^2 as roots, along with their entire conjugate group, so

$$g(x) = x^3 + x + 1.$$

Problem 4

(a) Determine the parameters of the BCH code correcting every double error over GF(8).

(b) Calculate the generator polynomial.

(c) Determine the codeword belonging to the message vector in which each component is 7.

Problem 4

(a) Determine the parameters of the BCH code correcting every double error over GF(8).

(b) Calculate the generator polynomial.

(c) Determine the codeword belonging to the message vector in which each component is 7.

Solution.

(a) Due to $t = 2$, the generator polynomial $g(x)$ must have roots y, y^2, y^3, y^4. We need to include the entire conjugate groups:

$$\{y, y^2, y^4\} \to x^3 + x + 1$$
$$\{y^3, y^5, y^6\} \to x^3 + x^2 + 1$$

so

$$g(x) = (x^3+x+1)(x^3+x^2+1) = x^6+x^5+x^4+x^3+x^2+x+1.$$

Problem 4

(a) $g(x)$ has degree $n - k = 6 \;\rightarrow\; n = 7, k = 1$.

($g(x)$ has roots $y^1, \ldots, y^6$, so this code can actually correct 3 errors, not just 2.)

Problem 4

(a) $g(x)$ has degree $n - k = 6 \;\rightarrow\; n = 7, k = 1$.

($g(x)$ has roots $y^1, \ldots, y^6$, so this code can actually correct 3 errors, not just 2.)

(b)

$$g(x) = (x^3+x+1)(x^3+x^2+1) = x^6+x^5+x^4+x^3+x^2+x+1.$$

Side remark. The generator matrix of this code is

$$G = [1\,1\,1\,1\,1\,1\,1].$$

Problem 4

(a) $g(x)$ has degree $n - k = 6 \rightarrow n = 7, k = 1$.

($g(x)$ has roots $y^1, \ldots, y^6$, so this code can actually correct 3 errors, not just 2.)

(b)

$$g(x) = (x^3+x+1)(x^3+x^2+1) = x^6+x^5+x^4+x^3+x^2+x+1.$$

Side remark. The generator matrix of this code is

$$G = [1\,1\,1\,1\,1\,1\,1].$$

(c) $u = (7) \rightarrow c = (7\,7\,7\,7\,7\,7\,7)$