

1. Let $n \in \mathbb{N}$ and $f(x) \in GF(q)[x]$. Then $f(x)$ generates a cyclic code C of length n over $GF(q)$, namely

$$C = \{\mathbf{c} \in GF(q)^n : \mathbf{c}(x) \equiv f(x)a(x) \pmod{x^n - 1} \text{ for some } a(x) \in GF(x)\}$$

Example : Let $n = 3, q = 2$ and $f(x) = 1 + x^2$. Then

$$\begin{aligned} C \pmod{x^3 - 1} &= \{(1 + x^2)a(x) \pmod{x^3 - 1} : a(x) \in GF(2)[x]\} \\ &= \{(1 + x^2)(a + bx + cx^2) \pmod{x^3 - 1} : a, b, c \in GF(2)\} \\ &= \{(a + b) + (b + c)x + (c + a)x^2 \pmod{x^3 - 1} : a, b, c \in GF(2)\} \\ &= \{0, x + x^2, 1 + x^2, 1 + x\} \pmod{x^3 - 1} \end{aligned}$$

Hence $C = \{000, 011, 101, 110\}$. So C is indeed cyclic with generator polynomial $1 + x$.

Find the generator polynomial of the binary cyclic code of length 5 generated by $1 + x + x^2 + x^3$.

Solution : We get that

$$\begin{aligned} C \pmod{x^5 - 1} &= \{(1 + x + x^2 + x^3)a(x) \pmod{x^5 - 1} : a(x) \in GF(2)[x]\} \\ &= \{(1 + x + x^2 + x^3)(a + bx + cx^2 + dx^3 + ex^4) \pmod{x^5 - 1} : a, b, c, d, e \in GF(2)\} \\ &= \{(a + e + d + c) + (b + a + e + d)x + (c + b + a + e)x^2 + (d + c + b + a)x^3 + \\ &\quad (e + d + c + b)x^4 : a, b, c, d, e \in GF(2)\} \end{aligned}$$

After some calculations, we get that the monic codeword polynomial of smallest degree is $1 + x$. So the generator polynomial of C is $1 + x$. □

2. Let C_1 and C_2 be cyclic codes of length n over $GF(q)$ with generator polynomials $g_1(x)$ and $g_2(x)$. Prove that $C_1 \subseteq C_2$ if and only if $g_2(x)$ divides $g_1(x)$.

Proof : Suppose first that $C_1 \subseteq C_2$. Since $g_1(x)$ is the generator polynomial of C_1 , we have that $g_1(x)$ is the codeword polynomial of some codeword $\mathbf{c} \in C_1$. So $g_1(x) = \mathbf{c}(x)$. But $C_1 \subseteq C_2$. So $\mathbf{c} \in C_2$. Since $g_2(x)$ is the generator polynomial of C_2 , we have that $g_2(x)$ divides $\mathbf{c}(x)$. Hence $g_2(x)$ divides $g_1(x)$.

Suppose next that $g_2(x)$ divides $g_1(x)$. Let $\mathbf{c} \in C_1$. Then $g_1(x)$ divides $\mathbf{c}(x)$. Since $g_2(x)$ divides $g_1(x)$, we have that $g_2(x)$ divides $\mathbf{c}(x)$. Hence $\mathbf{c} \in C_2$. So $C_1 \subseteq C_2$. □

3. Let C be a binary cyclic code of length n . Prove that the weight of every codeword in C is even if and only if $1 + x$ divides the generator polynomial of C .

Proof : Let $\mathbf{w} = (w_0, w_1, \dots, w_{n-1}) \in GF(2)^n$. Then $\mathbf{w}(x) = w_0 + w_1x + \dots + w_{n-1}x^{n-1}$. So

$$w_0 + w_1 + \dots + w_{n-1} = \mathbf{w}(1)$$

Hence we get

$$\begin{aligned} \text{the weight of } \mathbf{w} \text{ is even} &\iff w_0 + w_1 + \dots + w_{n-1} \text{ is an even integer} \\ &\iff \mathbf{w}(1) = 0 \text{ in } GF(2) \\ &\iff x + 1 = x - 1 \text{ divides } \mathbf{w}(x) \end{aligned}$$

Suppose first that the weight of every codeword in C is even. Since the generator polynomial $g(x)$ of C is a codeword polynomial, it follows from the above that $1 + x$ divides $g(x)$.

Suppose next that $1 + x$ divides the generator polynomial $g(x)$ of C . Let $\mathbf{c} \in C$. Then $g(x)$ divides $\mathbf{c}(x)$. Since $1 + x$ divides $g(x)$, we get that $1 + x$ divides $\mathbf{c}(x)$. So the weight of \mathbf{c} is even by the above. \square

Remark: There is another way of proving this exercise. Let C' be the binary code consisting of all words of even weight. Then C' is a cyclic code with generator polynomial $1 + x$. The exercise now follows from Ex. # 2.

4. Let $f(x) \in GF(q)[x]$ be a monic divisor of $x^n - 1$ and C the cyclic code of length n over $GF(q)$ generated by $f(x)$ (see Ex#1). Prove that $f(x)$ is the generator polynomial of C .

Proof : Let $g(x)$ be the generator polynomial of the cyclic code generated by $f(x)$. Since $f(x)$ is a codeword polynomial, we have that $g(x)$ divides $f(x)$.

Since $g(x)$ is a codeword polynomial and C is generated by $f(x)$, we have that

$$g(x) \equiv f(x)a(x) \pmod{x^n - 1}$$

for some polynomial $a(x) \in GF(q)[x]$. So $x^n - 1$ divides $f(x)a(x) - g(x)$. Hence

$$f(x)a(x) - g(x) = (x^n - 1)u(x)$$

and so

$$g(x) = a(x)f(x) - u(x)(x^n - 1)$$

for some polynomial $u(x) \in GF(q)[x]$. Since $f(x)$ divides $f(x)$ and $f(x)$ divides $x^n - 1$, we get that $f(x)$ divides $a(x)f(x) - u(x)(x^n - 1)$. So $f(x)$ divides $g(x)$.

We showed that $g(x)$ divides $f(x)$ and that $f(x)$ divides $g(x)$. This is only possible if

$$f(x) = \lambda g(x)$$

for some constant $\lambda \in GF(q)$. But $f(x)$ and $g(x)$ are both monic polynomials. So $\lambda = 1$ and $f(x) = g(x)$.

Hence $f(x)$ is the generator polynomial of the cyclic code generated by $f(x)$. \square

We now prove the more general case:

Let $f(x) \in GF(q)[x]$ be a polynomial and C the cyclic code of length n over $GF(q)$ generated by $f(x)$. Then the generator polynomial of C is $\gcd(f(x), x^n - 1)$.

Proof : Let $r(x)$ be the remainder of $f(x)$ divided by $x^n - 1$. Note that $\gcd(f(x), x^n - 1) = \gcd(r(x), x^n - 1)$ by the Euclidean Algorithm.

Let $g(x)$ be the generator polynomial of the cyclic code generated by $f(x)$. Since $r(x) \equiv f(x) \cdot 1 \pmod{x^n - 1}$ and $\deg(r(x)) < n$, we get that $r(x)$ is a codeword polynomial. So $g(x)$ divides $r(x)$. Since $g(x)$ divides $x^n - 1$, we get that $g(x)$ divides $\gcd(r(x), x^n - 1)$.

Since $g(x)$ is a codeword polynomial, we have that

$$g(x) \equiv f(x)a(x) \pmod{x^n - 1}$$

for some polynomial $a(x)$. Hence

$$g(x) = f(x)a(x) + (x^n - 1)b(x)$$

for some polynomial $b(x)$. Note that $\gcd(r(x), x^n - 1) = \gcd(f(x), x^n - 1)$ divides $f(x)$ and $\gcd(r(x), x^n - 1)$ divides $x^n - 1$. Hence $\gcd(r(x), x^n - 1)$ divides $f(x)a(x) + (x^n - 1)b(x)$. So $\gcd(r(x), x^n - 1)$ divides $g(x)$.

Since $g(x)$ divides $\gcd(r(x), x^n - 1)$ and $\gcd(r(x), x^n - 1)$ divides $g(x)$ and since $g(x)$ and $\gcd(r(x), x^n - 1)$ are monic, we have that $g(x) = \gcd(r(x), x^n - 1) = \gcd(f(x), x^n - 1)$. \square