

1. 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 $C_1 \subseteq C_2$. □

2. Prove that $f^*(x)$ divides $x^n - 1$ if $f(x)$ divides $x^n - 1$.

Proof : Suppose that $f(x)$ divides $x^n - 1$. Then

$$x^n - 1 = f(x)h(x) \tag{1}$$

for some polynomial $h(x)$. Put $k = \deg(f(x))$. Then

$$n = \deg(x^n - 1) = \deg(f(x)h(x)) = \deg(f(x)) + \deg(h(x)) = k + \deg(h(x))$$

and so $\deg(h(x)) = n - k$. Hence

$$f^*(x) = x^k f\left(\frac{1}{x}\right) \quad \text{and} \quad h^*(x) = x^{n-k} h\left(\frac{1}{x}\right)$$

In (1), we replace x by $\frac{1}{x}$ and multiply by x^n . We get that

$$1 - x^n = x^n \left(\frac{1}{x^n} - 1\right) = x^n f\left(\frac{1}{x}\right) h\left(\frac{1}{x}\right) = \left[x^k f\left(\frac{1}{x}\right)\right] \left[x^{n-k} h\left(\frac{1}{x}\right)\right] = f^*(x)h^*(x)$$

So

$$x^n - 1 = f^*(x)(-h^*(x))$$

Since $-h^*(x)$ is a polynomial, we have that $f^*(x)$ divides $x^n - 1$. □

3. 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

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

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

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

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 : In general, let $f(x) \in GF(q)[x]$ with $\deg(f(x)) < n$. Let $g(x)$ be the generator polynomial of the cyclic code generated by $f(x)$. Note that $f(x)$ is a codeword polynomial (namely put $q(x) = 1$). So $g(x)$ divides $f(x)$. Since $g(x)$ divides $x^n - 1$, we get that $g(x)$ divides $\gcd(f(x), x^n - 1)$.

One can prove that $g(x) = \gcd(f(x), x^n - 1)$ but we will not use that fact in this exercise.

So let $g(x)$ be the generator polynomial of the binary cyclic code of length 5 generated by $1 + x + x^2 + x^3$. Then $g(x)$ divides $\gcd(x^3 + x^2 + x + 1, x^5 - 1)$. Using the Euclidean Algorithm if needed, we easily find that

$$\gcd(x^3 + x^2 + x + 1, x^5 - 1) = x + 1$$

So $g(x) \in \{1, 1 + x\}$.

Suppose $g(x) = 1$. Then there exists $q(x) \in GF(2)[x]$ such that

$$1 \equiv (1 + x + x^2 + x^3)q(x) \pmod{x^5 - 1}$$

So $x^5 - 1 = x^5 + 1$ divides $(1 + x + x^2 + x^3)q(x) - 1$. Hence

$$(1 + x + x^2 + x^3)q(x) - 1 = u(x)(x^5 + 1)$$

and so

$$1 = u(x)(x^5 + 1) + q(x)(1 + x + x^2 + x^3)$$

for some $u(x) \in GF(2)[x]$. Since $x + 1$ divides $1 + x + x^2 + x^3$ and $x + 1$ divides $x^5 + 1$, we have that $1 + x$ divides $u(x)(x^5 + 1) + q(x)(1 + x + x^2 + x^3)$. So $1 + x$ divides 1, a contradiction.

Hence $g(x) \neq 1$. So $g(x) = 1 + x$. □

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#3). 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

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

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

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

and so

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

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 $q(x)f(x) - u(x)(x^n - 1)$. 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 $f(x)$. □