Math 525

Section 4.5: Dual Cyclic Codes

November 9, 2020

- **Main Result:** Let C be an (n, k) cyclic code with generator polynomial $g(x) \in K[x]$ and let $h(x) \in K[x]$ be such that $g(x)h(x) = x^n + 1$. Note that $\deg g = n - k$ and $\deg h = k$. Then $C^\perp$, the dual of C, is an $(n, n-k)$ cyclic code whose generator polynomial is equal to the reciprocal of the polynomial $h(x)$. That is, $g_{C^\perp}(x) = x^{\deg h} \cdot h(x^{-1}) = x^k h(x^{-1})$.
- For example, the reciprocal of $h(x) = x^4 + x + 1$ is equal to $x^4 \cdot (x^{-4} + x^{-1} + 1) = x^4 + x^3 + 1$.
- Let $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \in C$. We know that $c(x) = a(x)g(x)$ for some $a(x) = a_0 + a_1 x + \cdots + a_{k-1}x^{k-1}$.
- It follows that

$$c(x)h(x) = a(x)g(x)h(x) = a(x)(x^n + 1). \tag{1}$$

- The coefficients of $x^k, x^{k+1}, \ldots, x^{n-1}$ in $a(x)(x^n + 1)$ are all equal to zero. Hence, the same is true for the coefficients of $x^k, x^{k+1}, \ldots, x^{n-1}$ in $c(x)h(x)$.
- The coefficient of x^i in $c(x)h(x)$ is:

$$\sum_{j=0}^{k} h_j c_{i-j} = 0 \quad \text{for } k \le i \le n-1.$$

Expanding the above summations for $i = k, k+1, \ldots, n-1$, we get:

$$\begin{aligned} h_0 c_k + h_1 c_{k-1} + \cdots + h_{k-1} c_1 + h_k c_0 &= 0 \\ h_0 c_{k+1} + h_1 c_k + \cdots + h_{k-1} c_2 + h_k c_1 &= 0 \\ \vdots &= \vdots \\ h_0 c_{n-1} + \cdots + h_k c_{n-2-k} + h_k c_{n-1-k} &= 0. \end{aligned}$$

The above equations can be written in matrix form as $(c_0, c_1, \ldots, c_{n-1}) \cdot H = 0$ where:

$$H = \begin{bmatrix} h_k & 0 & 0 & \cdots & 0 \\ h_{k-1} & h_k & 0 & \cdots & 0 \\ h_{k-2} & h_{k-1} & h_k & & 0 \\ \vdots & h_{k-2} & h_{k-1} & & \vdots \\ \vdots & \vdots & h_{k-2} & & \vdots \\ \vdots & \vdots & \vdots & & h_k \\ \vdots & \vdots & \vdots & & h_{k-1} \\ h_0 & \vdots & \vdots & & h_{k-2} \\ 0 & h_0 & \vdots & & \vdots \\ \vdots & 0 & h_0 & & \vdots \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & h_0 \end{bmatrix}_{n \times n-k}$$

- Since $h_k \neq 0$, the $n-k$ columns of the above matrix H are linearly independent, that is, rank $H = n-k$. Thus, H is a parity-check for C.
- From $x^n + 1 = g(x)h(x)$, it follows that $x^{-n} + 1 = g(x^{-1})h(x^{-1})$. Multiplying both sides of this equality by x^n yields

$$x^n + 1 = \underbrace{x^{n-k} g(x^{-1})}_{\tilde{g}(x)} \cdot \underbrace{x^k h(x^{-1})}_{\tilde{h}(x)}$$

- The polynomial $\tilde{h}(x) = x^k h(x^{-1}) = h_k + h_{k-1}x + h_{k-2}x^2 + \cdots + h_0 x^{n-1}$ is the reciprocal of $h(x)$, and it is a divisor of $x^n + 1$.
- The transpose of H, namely,

$$\begin{bmatrix} \tilde{h}(x) \\ x\tilde{h}(x) \\ \vdots \\ x^{n-k-1}\tilde{h}(x) \end{bmatrix}$$

is the generator matrix of $C^{\perp}$. Since $\tilde{h}(x)$ is a divisor of $x^n + 1$, it follows that $C^{\perp}$ is a cyclic code with generator polynomial $g_{C^{\perp}}(x) = \tilde{h}(x)$.

In summary, we have:

Theorem (Theorem 4.5.2)

If C is an (n, k) cyclic code with generator polynomial $g(x)$, then $C^{\perp}$ is an $(n, n-k)$ cyclic code with generator polynomial

$$g_{C^{\perp}}(x) = \tilde{h}(x) = x^k h(x^{-1}),$$

where

$$h(x) = \frac{x^n + 1}{g(x)}.$$