# Math 525

## Section 4.3: Generator and Parity-Check Matrices for Cyclic Codes

November 4, 2020



Let $C$ be an $(n, k)$ cyclic code with generator polynomial $g(x) = g_0 + g_1 x + \cdots + g_{n-k} x^{n-k}$. Note that $g_0 = g_{n-k} = 1$ (why?).

A generator matrix for $C$ is the following $k \times n$ matrix $G$:

$$\begin{bmatrix} g_0 & g_1 & g_2 & \cdot & \cdot & \cdot & \cdot & \cdot & g_{n-k} & 0 & 0 & 0 & \cdot & \cdot & 0 \\ 0 & g_0 & g_1 & g_2 & \cdot & \cdot & \cdot & \cdot & \cdot & g_{n-k} & 0 & 0 & \cdot & \cdot & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & \cdot & \cdot & \cdot & \cdot & \cdot & g_{n-k} & 0 & \cdot & \cdot & 0 \\ \vdots & & & & & & & & & & & & & & \vdots \\ 0 & 0 & \cdot & \cdot & \cdot & 0 & g_0 & g_1 & g_2 & \cdot & \cdot & \cdot & \cdot & \cdot & g_{n-k} \end{bmatrix}$$

Sometimes we denote $G$ as $\begin{bmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-1}g(x) \end{bmatrix}$.

### Example

Consider the cyclic code of length 7 whose generator polynomial is $g(x) = 1 + x + x^3$. In this case, $n = 7$ and $k = 4$. A generator matrix for this code is

$$G = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}.$$



Let $C$ be an $(n, k)$ cyclic code $C$. The $k$ information digits $(a_0, a_1, \ldots, a_{k-1})$ are represented by

$$a(x) = a_0 + a_1 x + \cdots + a_{k-1} x^{k-1}.$$

**Encoding**: The vector $a = (a_0, a_1, \ldots, a_{k-1})$ is encoded as $aG$. In terms of polynomials, this is the same as $a(x)g(x)$.

Therefore, the encoding rule is: Let $a(x)$ be a polynomial of degree $\leq k - 1$. Then:

$$a(x) \text{ is encoded as } a(x) \cdot g(x).$$

## Parity-Check Matrix

Let $C$ be an $(n, k)$ cyclic code with generator polynomial $g(x)$. Recall: $r = (r_0, \dots, r_{n-1}) \in C$ if and only if $r(x) \bmod g(x) = 0$ where

$$r(x) = r_0 + r_1 x + \cdots + r_{n-1}x^{n-1}.$$

Saying that $r(x) \bmod g(x) = 0$ is equivalent to saying that

$$r_0 \bmod g(x) + r_1 x \bmod g(x) + \cdots + r_{n-k-1}x^{n-k-1}x^{n-k-1} \bmod g(x) +$$
$$r_{n-k}x^{n-k}x^{n-k} \bmod g(x) + \cdots + r_{n-1}x^{n-1}x^{n-1} \bmod g(x) = 0,$$

or $(r_0, \dots, r_{n-k-1}, r_{n-k}, \dots, r_{n-1}) \cdot H = 0$, where

$$H = \left[\begin{array}{c} 1 \bmod g(x) \\ x \bmod g(x) \\ \vdots \\ x^{n-k-1} \bmod g(x) \\ \hline x^{n-k} \bmod g(x) \\ \vdots \\ x^{n-1} \bmod g(x) \end{array}\right] = \left[\begin{array}{c} 1 \\ x \\ \vdots \\ x^{n-k-1} \\ \hline x^{n-k} \bmod g(x) \\ \vdots \\ x^{n-1} \bmod g(x) \end{array}\right] = \left[\begin{array}{c} I_{n-k} \\ \hline X \end{array}\right].$$

Since $H$ has rank equal to $k$, it is a parity-check matrix for $C$.



## Parity-Check Matrix (Cont'd.)

### Example

Find a parity-check matrix for the cyclic code of length 7 and with generator polynomial $g(x) = 1 + x + x^3$.

**Remarks**:

1. The syndrome of a received polynomial $r(x)$ equals $r(x) \bmod g(x)$.
2. Another generator matrix is $G = [X|I_k]$. In many textbooks, this is called a systematic generator matrix.