

ECE 590: Error Correcting Codes

Lecture: Introduction to Cyclic Codes

Henry D. Pfister

Department of Electrical and Computer Engineering
Duke University

Definition 1 (Cyclic Shift).

A **cyclic** (or circular) right shift of a vector is formed by moving each vector element to the right and wrapping the last element around to the first element. For example, a right cyclic shift maps

$$(x_0, x_1, \dots, x_{n-1}) \longrightarrow (x_{n-1}, x_0, x_1, \dots, x_{n-2}).$$

Definition 2 (Cyclic Code).

A **cyclic code** over \mathbb{F} is a linear code over \mathbb{F} where any cyclic shift of a codeword is also a codeword.

Example 3 (The Simplex Code).

Consider the $(7, 3)$ binary linear code whose 8 codewords are

$$\mathcal{C} = \{0000000, 1011100, 0101110, 1110010, \\ 0010111, 1001011, 0111001, 1100101\}$$

It is cyclic because all n.z. codewords are cyclic shifts of 1011100.

Its cyclic structure can also be seen in the fact that it has Toeplitz generator matrix

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

Why Cyclic Codes?

Cyclic codes have a close connection to polynomial arithmetic that allows efficient encoding and decoding.

Definition 4 (Polynomial Representation).

For an (n, k) cyclic code, the codeword $\underline{c} = (c_0, c_1, \dots, c_{n-1})$ and message vector $\underline{m} = (m_0, m_1, \dots, m_{k-1})$ are associated with the polynomials

$$c(x) = \sum_{i=0}^{n-1} c_i x^i \quad m(x) = \sum_{i=0}^{k-1} m_i x^i.$$

Definition 5 (Generator Polynomial).

The **generator polynomial** $g(x)$ is monic with degree $n-k$. For each codeword $c(x) \in \mathcal{C}$, there is a message $m(x)$ such that

$$c(x) = g(x)m(x).$$

The Generator Polynomial

Choosing $m(x) = 1$ shows that $g(x)$ is the unique monic codeword polynomial of minimal degree.

Example 6.

The generator polynomial for the $(7, 3)$ binary code in the previous example is $g(x) = 1 + x^2 + x^3 + x^4$ and $\deg(g(x)) = 7 - 4 = 3$. Since $m(x)$ has degree at most $k - 1$, we can verify that

$$\deg(c(x)) = \deg(g(x)) + \deg(m(x)) \leq n - 1.$$

Based on this, we see that entire code is given by

$$\mathcal{C} = \{g(x)m(x) \mid m(x) \in \mathbb{F}[x], \deg(m(x)) \leq k - 1\}$$

Definition 7 (Polynomial Division).

For a polynomial $a(x)$ and divisor $d(x) \neq 0$, the **remainder** $r(x)$ and **quotient** $q(x)$ are uniquely defined by $\deg(r(x)) < \deg(d(x))$ and

$$a(x) = q(x)d(x) + r(x).$$

Definition 8 (Polynomial Modulo).

In discrete mathematics, the **polynomial modulo** operation

$$r(x) = a(x) \bmod d(x)$$

is used to represent the remainder $r(x)$ of division by $d(x)$.

Lemma 9 (Properties of Modulo).

Reduction modulo $x^n - 1$ is equivalent to the identity $x^n = 1$, and $x^j \bmod (x^n - 1) = x^{j \bmod n}$. Also, the modulo operation is linear.

Corollary 10 (Modulo $x^n - 1$ Cyclic Shift Property).

From this, we get

$$\begin{aligned}x^j c(x) \bmod x^n - 1 &= \left(\sum_{i=0}^{n-1} c_i x^{i+j} \right) \bmod (x^n - 1) \\ &= \sum_{i=0}^{n-1} c_i (x^{i+j} \bmod (x^n - 1)) \\ &= \sum_{i=0}^{n-1} c_i x^{(i+j) \bmod n}\end{aligned}$$

The Parity-Check Polynomial

Theorem 11 (The Parity-Check Polynomial).

For an (n, k) cyclic code, the generator $g(x)$ must divide $x^n - 1$ and the quotient $h(x) = (x^n - 1)/g(x)$ is called the **parity-check polynomial**. For any codeword $c(x)$, it follows that $h(x)$ satisfies

$$h(x)c(x) \bmod (x^n - 1) = 0.$$

Proof.

Since $h(x)$ is given by dividing $x^n - 1$ by $g(x)$, one can prove this statement by observing that $c(x) = m(x)g(x)$ for some $m(x)$ and, hence,

$$h(x)c(x) = m(x)g(x)h(x) = m(x)(x^n - 1).$$

Since $x^n - 1$ divides $h(x)c(x)$, the remainder is zero. □

The Parity-Check Polynomial

Example 12.

The generator and parity-check polynomials for the simplex code are $g(x) = 1 + x^2 + x^3 + x^4$ and $h(x) = 1 + x^2 + x^3$. Thus, we compute

$$g(x)h(x) = (1 + x^2 + x^3 + x^4)(1 + x^2 + x^3) = 1 + x^7.$$

Example 13 (binary Hamming codes).

The binary Hamming codes are (n, k) cyclic codes, with $n = 2^r - 1$ and $k = n - r$, that correct all single errors. A primitive polynomial of degree- r generates such a code. For $r = 3, 4, 5$, we get

$$\begin{aligned}(7, 4) \quad & g(x) = 1 + x^2 + x^3 \\(15, 11) \quad & g(x) = 1 + x^3 + x^4 \\(31, 26) \quad & g(x) = 1 + x^3 + x^5.\end{aligned}$$

Definition 14 (Cyclic Generator Matrix).

The generator polynomial $g(x) = g_0 + g_1x + g_2x^2 + \cdots + g_{n-k}x^{n-k}$ of an (n, k) cyclic code has a **cyclic generator matrix** of the form

$$\underline{G} = \begin{bmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & 0 & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k} & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & 0 & 0 & g_0 & \cdots & g_{n-k-1} & g_{n-k} \end{bmatrix}.$$

The encoding $\underline{c} = \underline{m}\underline{G}$ is identical to $c(x) = m(x)g(x)$. Using $[\underline{G}]_{ij} = g_{j-i}$ for $0 \leq i \leq j \leq n-1$ and 0 otherwise, we have

$$\begin{aligned} c(x) &= \sum_{j=0}^{n-1} x^j c_j = \sum_{j=0}^{n-1} x^j \sum_{i=0}^{k-1} m_i [\underline{G}]_{ij} = \sum_{j=0}^{n-1} x^j \sum_{i=0}^{k-1} m_i g_{j-i} \\ &= \sum_{i=0}^{k-1} m_i x^i \sum_{j=i}^{n-1} x^{j-i} g_{j-i} = \sum_{i=0}^{k-1} m_i x^i g(x) = m(x)g(x). \end{aligned}$$

Definition 15 (Cyclic Parity-Check Matrix).

The parity-check polynomial $h(x) = h_0 + h_1x + h_2x^2 + \cdots + h_kx^k$ of an (n, k) code has a **cyclic parity-check matrix** of the form

$$\underline{H} = \begin{bmatrix} h_k & h_{k-1} & \cdots & h_0 & 0 & 0 & 0 \\ 0 & h_k & h_{k-1} & \cdots & h_0 & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & 0 & 0 & h_k & \cdots & h_1 & h_0 \end{bmatrix}.$$

In this case, one can use the fact that $g(x)h(x) = x^n - 1$ to verify that $GH^T = 0$.

Systematic Encoding

For cyclic codes, the encoding $c(x) = m(x)g(x)$ is not systematic. One can overcome this by choosing

$$c(x) = p(x) + x^{n-k}m(x),$$

where the message $m(x)$ appears as the last k bits of $c(x)$ and the **parity polynomial** $p(x) = p_0 + p_1x + \cdots + p_{n-k-1}x^{n-k-1}$ has degree $\deg(p(x)) \leq n - k - 1$.

Theorem 16 (Systematic Encoding).

$p(x) \triangleq -x^{n-k}m(x) \bmod g(x)$ defines a systematic encoding.

Proof.

It is easy to see that $c(x)$ has the message as the last k bits. To see that it is a codeword, we compute $c(x) \bmod g(x)$

$$\begin{aligned} &= p(x) \bmod g(x) + x^{n-k}m(x) \bmod g(x) \\ &= -x^{n-k}m(x) \bmod g(x) + x^{n-k}m(x) \bmod g(x) = 0 \end{aligned}$$

Example 17.

Consider our example $(7, 3)$ code with $g(x) = 1 + x^2 + x^3 + x^4$. The message $\underline{m} = [0 \ 1 \ 1]$ is associated with the message polynomial $m(x) = x + x^2$ and the systematic encoding equation says that

$$p(x) = -x^4 m(x) \bmod g(x) = -x^5 - x^6 \bmod (1 + x^2 + x^3 + x^4).$$

To compute $p(x)$, we proceed by using polynomial long division to see that

$$\frac{x^5 + x^6}{1 + x^2 + x^3 + x^4} = (x^2 + 1) + \frac{x^3 + 1}{1 + x^2 + x^3 + x^4}$$

This implies that $p(x) = x^3 + 1$ and $c(x) = 1 + x^3 + x^5 + x^6$. One can verify that this is a codeword by observing that $(1 + x^2)(1 + x^2 + x^3 + x^4) \bmod 2 = 1 + x^3 + x^5 + x^6$.

The Syndrome Polynomial

When $c(x)$ is transmitted, the **received polynomial**

$$r(x) = \sum_{i=0}^{n-1} r_i x^i \quad \leftrightarrow \quad \underline{r} = (r_0, r_1, \dots, r_{n-1})$$

is defined by $r(x) = c(x) + e(x)$ and the **error polynomial** is

$$e(x) = \sum_{i=0}^{n-1} e_i x^i \quad \leftrightarrow \quad \underline{e} = (e_0, e_1, \dots, e_{n-1})$$

Definition 18 (Syndrome Polynomial).

The **syndrome polynomial** $s(x) = s_0 + s_1x + \dots + s_{n-k-1}x^{n-k-1}$ is

$$s(x) \triangleq r(x) \bmod g(x)$$

This definition provides a natural coset decomposition of all received polynomials because $r(x) = q(x)g(x) + s(x)$.

Definition 19 (Burst Error).

A **cyclic burst error** of length ℓ is a cyclic shift of an error pattern that has errors only in the first ℓ positions. Any such error can be written in the form $e(x) = x^i b(x) \bmod x^n - 1$ with $\deg(b(x)) < \ell$.

Theorem 20 (Burst Error Correction of Cyclic Codes).

A cyclic code generated by $g(x)$ can detect all error patterns consisting of a single cyclic burst error of length $\ell \leq \deg(g(x))$.

Proof.

Let $e(x) = x^i b(x)$ and suppose $s(x) = e(x) \bmod g(x) = 0$. Then, $x^i b(x) = q(x)g(x)$ and x^i must divide $q(x)$ because $g(x)$ is not divisible by x (e.g., it is the minimal degree codeword). But, $b(x) = (x^{-i}q(x))g(x)$ implies $\deg(b(x)) \geq \deg(g(x))$ and contradicts $\deg(b(x)) < \ell \leq \deg(g(x))$. Therefore, $s(x) \neq 0$.

