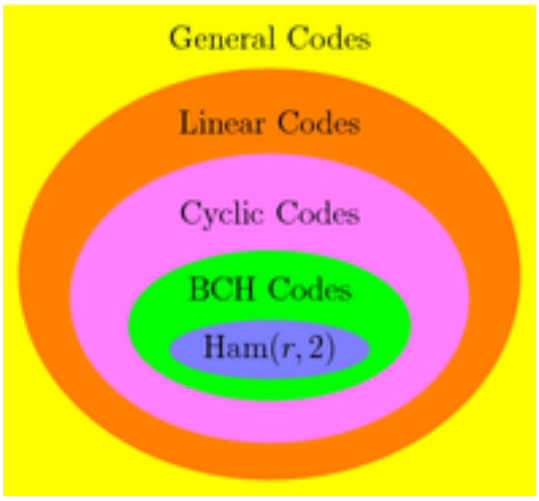
Math 525

Sections 4.1–4.2: Cyclic Codes

October 28, 2020

Code Hierarchy:



- Cyclic codes form a subclass of linear codes. They are used in many communication systems because they are easier to implement than general linear codes with no cyclic structure. That is, the cost of the encoding and decoding processes is smaller for cyclic codes.

- In this chapter, we will see:
  1. Basic theory of cyclic codes via their polynomial description.
  2. Generator and parity-check matrices for cyclic codes.
  3. Method for finding cyclic codes of a given length.
  4. The dual of a cyclic code.

- So far, we have represented messages and codewords by vectors. However, for cyclic codes it is common practice to represent messages and codewords by polynomials.

- We will now review the basic facts about polynomials that will be needed. The division algorithm for polynomials plays a central role.

Definition

A polynomial over the field $K = \{0, 1\}$ is an expression of the form

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

where n is any nonnegative integer and $a_i \in K$. The element x is called an indeterminate. The set of all such polynomials is denoted by $K[x]$.

Definition

Consider the polynomial

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in K[x],$$

and assume that $a_n \neq 0$. Then a_n is called the leading coefficient of $f(x)$, and the degree of $f(x)$, denoted by $\deg f(x)$, is equal to n. The constant polynomial $f(x) = 0$ does not have a degree.

Note: It follows from the definition that the degree of $f(x) = 1$ is equal to zero.

- Polynomials over K are added and multiplied just like polynomials over $\mathbb{R}$ (the real numbers), except that the coefficients are added and multiplied in K.
- For example, let $f(x) = x^3 + x + 1$ and $g(x) = x^4 + x^2 + x$ be two polynomials with coefficients in $K[x]$. Then

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

Also,

$$f(x) \cdot g(x) = x^7 + x^3 + x.$$

- Let $f(x), g(x) \in K[x]$. Then:
  1. If $f(x) \neq g(x)$, then $\deg(f(x) + g(x)) \leq \max\{\deg f(x), \deg g(x)\}$.
  2. $\deg(f(x) \cdot g(x)) = \deg f(x) + \deg g(x)$.

Properties: For all $f(x), g(x) \in K[x]$, one has:

1. $(f(x) + g(x))^2 = f(x)^2 + g(x)^2$, a.k.a. *freshman's dream*.
2. $(f(x) + g(x))^4 = f(x)^4 + g(x)^4$.
3. $(f(x) + g(x))^{2^r} = f(x)^{2^r} + g(x)^{2^r}$, for $r \geq 1$.
4. $f(x)^2 = f(x^2)$.

Theorem (The Division Algorithm for Polynomials)

Let $f(x)$ and $g(x)$ be two polynomials in $K[x]$ with $g(x) \neq 0$. Then there exist unique polynomials $q(x)$ (the quotient) and $r(x)$ (the remainder) such that

$$f(x) = g(x)q(x) + r(x)$$

where either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

- The quotient $q(x)$ and the remainder $r(x)$ can be found via long division.
- Example: What is the quotient and remainder when $x^5 + x^3 + x + 1$ is divided by $x^3 + x^2 + x + 1$?
- Observe that if $\deg f(x) < \deg g(x)$, then we can immediately conclude that $q(x) = 0$ and $r(x) = f(x)$.

* * *

Words as polynomials:
Let $v = (v_0, v_1, \ldots, v_{n-1}) \in K^n$. We can represent v by the polynomial

$$v(x) = v_0 + v_1 x + \cdots + v_{n-1} x^{n-1} \in K[x],$$

and vice-versa. Notation: $v \leftrightarrow v(x)$.

So a code C of length n can be represented as a set of polynomials of degree less than or equal to $n - 1$.

Definition

If $r(x)$ is the remainder when $f(x)$ is divided by $h(x)$, then we write: $f(x) \bmod h(x) = r(x)$. For convenience, we use the notation $[f(x)]_{h(x)}$ as a shorthand for $f(x) \bmod h(x)$.

Lemma

Suppose $[f(x)]_{h(x)} = r(x)$ *and* $[g(x)]_{h(x)} = s(x)$. *Then:*

1. $$\begin{aligned} [f(x) + g(x)]_{h(x)} &= r(x) + s(x) \\ &= [f(x)]_{h(x)} + [g(x)]_{h(x)}. \end{aligned}$$
2. $$\begin{aligned} [f(x) \cdot g(x)]_{h(x)} &= [r(x) \cdot s(x)]_{h(x)} \\ &= [\,[f(x)]_{h(x)} \cdot [g(x)]_{h(x)}\,]_{h(x)}. \end{aligned}$$

Definition

If $f(x)$ and $g(x)$ leave the same remainder when divided by $h(x)$, then we write: $f(x) \equiv g(x) \pmod{h(x)}$. And we say: "$f(x)$ is equivalent (or congruent) to $g(x)$ modulo $h(x)$."

Example

Let $f(x) = x^5 + x^3 + x + 1$, $g(x) = x^6 + x^4 + x^3 + x^2$, and $h(x) = x^3 + x^2 + x + 1$. Then

$$f(x) \bmod h(x) = x^2 + x = g(x) \bmod h(x),$$

so $f(x) \equiv g(x) \pmod{h(x)}$.

Remark: $f(x) \equiv g(x) \pmod{h(x)}$ iff $f(x) + g(x) = k(x) \cdot h(x)$.

Lemma

Suppose $f(x) \equiv g(x) \pmod{h(x)}$. *Then:*

1. $f(x) + p(x) \equiv g(x) + p(x) \pmod{h(x)}$,
2. $f(x) \cdot p(x) \equiv g(x) \cdot p(x) \pmod{h(x)}$, *and*
3. $f(x)^n \equiv g(x)^n \pmod{h(x)}$ *for any positive integer* n.

Attention: Dividing both sides of the congruence by a common polynomial is usually not allowed. For example,

$$x \cdot (x+1) \equiv (x^2+1) \cdot (x+1) \pmod{x^3+1},$$

but

$$x \not\equiv x^2 + 1 \pmod{x^3+1}.$$

Definition

A linear code C is said to be cyclic if

$$v = (v_0, v_1, \ldots, v_{n-1}) \in C \Longrightarrow \pi(v) = (v_{n-1}, v_0, v_1, \ldots, v_{n-2}) \in C.$$

For any $w \in K^n$, $\pi(w)$ is called the cyclic shift of w.

Example: The codes

$$\{000, 110, 101, 011\} \text{ and } \{0000, 1010, 0101, 1111\}$$

are cyclic.

Lemma

$\pi(v + w) = \pi(v) + \pi(w)$ and $\pi(av) = a\pi(v)$ for all $v, w \in K^n$ and all $a \in K$.

In conclusion: π is a linear transformation of K^n. Thus, to show that a linear code C is cyclic, it is enough to show that $\pi(v) \in C$ for all v in a basis for C.

The smallest cyclic code containing a word $v = (v_0, v_1, \ldots, v_{n-1})$ is $C = \langle S \rangle$ where

$$S = \{v, \pi(v), \pi^2(v), \ldots, \pi^{n-1}(v)\}$$

and $\pi^i(v) = \underbrace{\pi \circ \pi \circ \cdots \circ \pi}_{i \text{ times}}(v)$.

Note that $\pi^n(v) = v$, for all $v \in K^n$.

Example

The smallest cyclic code of length 7 containing $v = 1001011$ is $C = \langle S \rangle$, where

$$S = \{1001011, 1100101, 1110010, 0111001, 1011100, 0101110, 0010111\}.$$

As an exercise, show that C is a $(7, 3)$ linear code with generating matrix

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

The relationship between cyclic codes and polynomials comes from the observation that:

$$\text{If } v \leftrightarrow v(x), \text{ then } \pi(v) \leftrightarrow x \cdot v(x) \bmod (x^n + 1). \quad (*)$$

The proof is by direct inspection:

$$x \cdot v(x) = v_0 x + v_1 x^2 + \cdots + v_{n-1} x^n.$$

So, $x \cdot v(x) \bmod (x^n + 1) =$

$$(v_0 x + v_1 x^2 + \cdots + v_{n-2} x^{n-1} + v_{n-1} x^n) \bmod (x^n + 1).$$

Since $x^n \bmod (x^n + 1) = 1$, it follows that the latter expression is equal to

$$\begin{aligned} v_0 x + v_1 x^2 + \cdots + v_{n-2} x^{n-1} + v_{n-1} &= \\ v_{n-1} + v_0 x + v_1 x^2 + \cdots + v_{n-2} x^{n-1} &= \pi(v)(x). \end{aligned}$$

Hence, $\pi(v)(x) = x \cdot v(x) \bmod (x^n + 1)$. □

Example

$v = 1101$ corresponds to $v(x) = 1 + x + x^3$. Note:

$$x \cdot (1 + x + x^3) = x + x^2 + x^4.$$

Now, $x + x^2 + x^4 \bmod (x^4 + 1) = 1 + x + x^2$, which in turn corresponds to $1110 = \pi(v)$. □

As a consequence of the previous observation and the lemma on slide #8, note that if $v(x) \in C$ (a cyclic code of length n), then:

1. $\pi^i(v)(x) = (x^i \cdot v(x)) \bmod (x^n + 1) \in C$ for all $i \geq 0$;
2. $(a(x) \cdot v(x)) \bmod (x^n + 1) \in C$ for any $a(x) \in K[x]$.

These remarks are Lemma 4.2.12. Note: For any $w(x) \in K[x]$ of degree $< n$,

$$(x^n \cdot w(x)) \bmod (x^n + 1) = w(x)$$

and, more generally, for any $i \geq 0$,

$$(x^i \cdot w(x)) \bmod (x^n + 1) = (x^{i \bmod n} \cdot w(x)) \bmod (x^n + 1).$$

Now we will define the generator polynomial for a cyclic code C. All properties of C as well the implementation of C depend on that polynomial.

Definition

Let C be a cyclic code. A nonzero polynomial $g(x) \in C$ of lowest degree is called a generator polynomial for C.

Remark: $g(x)$ is unique, so it is actually "the" nonzero polynomial of lowest degree in C.

Example: Consider the following binary cyclic code of length 7:

0000000,	0110100,	0011010,	0101110,
1000110,	1110010,	1011100,	1101000,
1100101,	1010001,	1111111,	1001011,
0100011,	0010111,	0111001,	0001101.

The generator polynomial for C is $g(x) = 1 + x + x^3$.

The two main properties of generator polynomials are given by the following:

Theorem (Theorem 4.2.13, part 3)

Let C be a cyclic code of length n and with generator polynomial $g(x)$. Then:

$$c(x) \in C \iff c(x) = a(x) \cdot g(x)$$

for some $a(x) \in K[x]$ with $\deg a(x) < n - \deg g(x)$.

Theorem (Theorem 4.2.13, parts 1 and 2)

With the above notation, suppose $\deg g(x) = r$. *Then:*

1. $\dim C = k = n - r$.
2. $\{g(x), x \cdot g(x), \ldots, x^{k-1} \cdot g(x)\}$ *is basis for* C.

Idea for the proof: Show that any $c(x) \in C$ can be written as a linear combination of $g(x), x \cdot g(x), \ldots, x^{n-r-1} \cdot g(x)$, and then show that these elements are linearly independent. □

The following theorem completely characterizes cyclic codes of length n:

Theorem (Theorem 4.2.17)

A polynomial $g(x) \in K[x]$ *is the generator polynomial for a cyclic code of length* n *if and only if* $g(x) \mid x^n + 1$.

Remark: *We say that* $b(x) \in K[x]$ *is a divisor of* $a(x) \in K[x]$, *or* $b(x)$ *divides* $a(x)$, *if* $a(x) = b(x) \cdot c(x)$ *for some* $c(x)$ *in* $K[x]$. *Notation:* $b(x) \mid a(x)$.

Idea for the proof of Thm. 4.2.17: For $\Rightarrow$, long divide $x^n + 1$ by $g(x)$ and show that the remainder is zero. For $\Leftarrow$, consider the cyclic code

$$C = \{a(x) \cdot g(x) \bmod (x^n + 1) \mid a(x) \in K[x]\}$$

of length n, and show that $g(x)$ has the smallest degree among all nonzero polynomials in C. □

Why is the above theorem important?

Like integers can be factored uniquely as a product of *prime numbers*, polynomials in $K[x]$ can be factored uniquely as a product of *irreducible polynomials*.

We say that a polynomial $f(x) \in K[x]$ is irreducible if its only divisors are 1 and itself.

Important conclusion: Theorem 4.2.17 actually states that once the factorization of $x^n + 1 \in K[x]$ into *irreducibles* is known, all cyclic codes of length n are determined. The Maple command

$$\text{Factor}(x^n + 1) \bmod 2;$$

can be used to find the factorization of $x^n + 1 \in K[x]$ into irreducibles.

Question: Given $v(x) \in K[x]$ of degree $\leq n - 1$, what is the generator polynomial for the smallest cyclic code containing $v(x)$?

Corollary (Corollary 4.2.18)

The generator polynomial for the smallest cyclic code of length n containing $v(x)$ (as above) is

$$g(x) = \gcd(v(x), x^n + 1).$$

The greatest common divisor between two polynomials can be efficiently calculated with the Euclidean algorithm, see Appendix A. Or, you can use Wolfram Cloud:

$$\text{PolynomialGCD}[x^7 + 1, x^4 + x^2 + x, \text{ Modulus} \to 2]$$

The result in the above case is $x^3 + x + 1$.