Math 525

Section 4.4: Finding Cyclic Codes

November 6, 2020

- **Our objective:** Given $n \geq 2$, describe all cyclic codes of length n. By "describe," we mean determine the generator polynomial.
- In view of Theorem 4.2.17, a cyclic code of length n and dimension k can be described once we have a factor of $x^n + 1$ of degree $n - k$. For example, let $n = 7, k = 3$, and assume that the factorization

$$x^7 + 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)$$

  is given. Then $g(x) = (x + 1)(x^3 + x + 1) = x^4 + x^3 + x^2 + 1$ generates such a code. Another possibility is $g(x) = (x + 1)(x^3 + x^2 + 1)$ and so on.
- Having the *irreducible* factors of $x^n + 1$ at our disposal helps us achieve our objective. We say that $f(x) \in K[x]$ is irreducible if $f(x)$ cannot be written (or factored) as a product of polynomials whose degrees are strictly smaller than the degree of $f(x)$.
- Two obvious factors of $x^n + 1$ are 1 and $x^n + 1$. The constant polynomial generates the universal code K^n of length n, whereas $x^n + 1$ generates $\{\mathbf{0}\}$, where $\mathbf{0}$ is the all-zero codeword of length n. These "uninteresting" cyclic codes are called the improper cyclic codes of length n. All other cyclic codes of length n are called proper cyclic codes of length n.

Example

Find the factorizations of x^3+1 and x^6+1 into irreducible factors.

Theorem

If $n = 2^r \cdot s$, then $x^n + 1 = (x^s+1)^{2^r}$.

Corollary

Let $n = 2^r \cdot s$ where s is odd and let $x^s + 1 = f_1(x)\cdots f_z(x)$, where $f_1(x),\dots,f_z(x)$ are distinct and irreducible. Then there are $(2^r+1)^z$ cyclic codes of length n and $(2^r+1)^z - 2$ proper cyclic codes of length n.

A result from abstract algebra (outside the scope of this course) states that if $p(x)$ is a polynomial, $p'(x)$ is its derivative, and $\gcd(p(x), p'(x)) = 1$, then $p(x)$ has no repeated roots. If n is odd, then

$$\frac{d}{dx}(x^n+1) = nx^{n-1} = x^{n-1}.$$

Since $\gcd\left(x^n+1, \frac{d}{dx}(x^n+1)\right) = 1$, it follows that x^n+1 has n distinct roots. *Hence, no repeated factors appear in the factorization of x^n+1 when n is odd.*

Idempotent Polynomials

From this point on, assume that n is odd. We will describe all cyclic codes of length n without having the factorization of x^n+1 at our disposal. For this, we will need the concept of *idempotent polynomials*.

Definition

A polynomial $I(x) \in K[x]$ of degree $< n$ is called an idempotent mod (x^n+1) if

$$I(x) \equiv I(x)^2 \pmod{x^n+1}.$$

Example

$I(x) = x + x^2 + x^4$ is an idempotent modulo x^7+1.

Idempotent Polynomials

Theorem (Theorem 4.4.13)

Let C be a cyclic code of length n. Then C contains exactly one idempotent code-polynomial $e(x)$ such that

$$C = \langle e(x), xe(x) \bmod (x^n+1), x^2e(x) \bmod (x^n+1), \ldots, x^{n-1}e(x) \bmod (x^n+1)\rangle.$$

Conclusion:

1. C is the smallest cyclic code containing $e(x)$. From Corollary 4.2.18, it follows that the generator polynomial for C is
$$g(x) = \gcd(e(x), x^n+1). \tag{1}$$
2. If we have an efficient method for producing all idempotents mod (x^n+1), then we can, via (1), determine all cyclic codes of length n.

Idempotent Polynomials

We will now develop a method for finding all idempotents mod (x^n+1). Keep in mind that n is assumed to be odd.

Recall: $I(x) \equiv I(x)^2 \pmod{x^n+1}$, so $I(x) \equiv I(x^2) \pmod{x^n+1}$. Therefore, if x^a is one of the terms of $I(x)$, then

$$x^{2a \bmod n},\ x^{4a \bmod n},\ x^{8a \bmod n},\ \text{etc.},$$

must all be terms of $I(x)$ as well.

The latter observation motivates us to partition $Z_n = \{0, 1, \ldots, n-1\}$ into "classes." Define:

$$C_i = \{i \cdot 2^j \pmod{n},\ \ j = 0, 1, \ldots, r\} \quad \text{where} \quad 2^r \bmod n = 1.$$

We have: $C_i \cap C_\ell$ is either the empty set or $C_i \cap C_\ell = C_i = C_\ell$.

Example

Construct all the classes modulo 7 and all the classes modulo 15.

Idempotent Polynomials

Note that

$$c_i(x) = \sum_{j \in C_i} x^j$$

is an idempotent polynomial corresponding to class C_i. Finally, any idempotent mod $(x^n + 1)$ can be written as:

$$\sum_{k=1}^{N} a_{i_k} c_{i_k}(x),$$

where N = number of distinct classes, $c_{i_k}(x)$ is the idempotent corresponding to class C_{i_k}, and $a_{i_k} \in \{0, 1\}$.

Example

Use the previous example to construct all the idempotents modulo $x^7 + 1$ and all the idempotents modulo $x^{15} + 1$. Then determine the number of cyclic codes of length 7 and the number of cyclic codes of length 15.

Example

Determine the generator polynomial for each cyclic code found in the previous example. *Hint*: See (1) on Slide #5.

Appendix: Proof of Theorem 4.4.13

Let $g(x)$ be the generator polynomial for C. Since $g(x)|x^n + 1$, then $x^n + 1 = g(x)h(x)$ for some polynomial $h(x)$. Since n is odd, $g(x)$ and $h(x)$ are relatively prime in the sense that their only common divisor is 1. By the Euclidean algorithm, the greatest common divisor of two polynomials can always be expressed as a linear combination of the two polynomials. Thus, there exist polynomials $t(x)$ and $s(x)$ such that

$$t(x)g(x) + s(x)h(x) = 1. \tag{2}$$

Example

Let $g(x) = (x + 1)(x^3 + x + 1)$ and $h(x) = x^3 + x^2 + 1$, so $g(x)h(x) = x^7 + 1$. Then

$$\underbrace{(x^2 + 1)}_{t(x)} \cdot g(x) + \underbrace{x^3}_{s(x)} \cdot h(x) = 1.$$

If we multiply both sides of (2) by $t(x)g(x)$, we obtain

$$(t(x)g(x))^2 + s(x)t(x)(x^n + 1) = t(x)g(x),$$

whence $(t(x)g(x))^2 \equiv t(x)g(x) \pmod{x^n + 1}$. This shows that $e(x) = [t(x)g(x)]_{(x^n+1)}$ is an idempotent. Moreover, $e(x) \in C$.

Appendix: Proof of Theorem 4.4.13 (Cont'd.)

The smallest cyclic code of length n containing $e(x)$ has generator polynomial equal to

$$\begin{aligned}\gcd(e(x), x^n+1) &= \gcd(x^n+1, t(x)g(x) \bmod (x^n+1)) \\ &= \gcd(x^n+1, t(x)g(x)) = g(x).\end{aligned}$$

Finally, the idempotent $e(x)$ satisfies $e(x)c(x) \equiv c(x) \pmod{x^n+1}$ for all $c(x) \in C$ (this follows from $e(x) = [1 - s(x)h(x)]_{(x^n+1)}$. If $e'(x)$ is another idempotent polynomial of C, then $e(x) = e'(x) \equiv [e(x)e'(x)]_{(x^n+1)}$. Hence the idempotent polynomial of C is unique. $\square$