Mathematics 392 – Seminar in Coding Theory
Discussion 4 – Generator Polynomials of Cyclic Codes
March 18, 2002

Background

Many of the codes that have been used in applications such as the CD audio system are *cyclic* codes because their "extra structure" that facilitates encoding and decoding. We will largely focus on these for the remainder of the Coding Theory Seminar. The most basic way to say what a cyclic code is to say that it is a linear code where the set of codewords is *closed under cyclic permutations.* We have seen in class that the algebra of polynomials is very useful to describe these codes. This is true because if we make the digits from a codeword of length n the coefficients of a polynomial $c(x)$ of degree $\leq n-1$, then the cyclic permutation is achieved by taking the remainder of $xc(x)$ on division by x^n+1.

The *generator polynomial* $g(x)$ of a cyclic code C is the nonzero polynomial of minimal degree corresponding to a codeword. We have seen the following key facts about generator polynomials:

- If $c(x)$ is any codeword polynomial of C, then $g(x)|c(x)$.
- $\deg(g) = n-k$, and the polynomials in $\{g(x), xg(x), \ldots, x^{k-1}g(x)\}$ form a basis for C.
- $g(x)|(x^n+1)$, where n is the blocklength.

Today we want to see how generator polynomials for cyclic codes can be used to work with these codes and consider how *all* cyclic codes of a given blocklength might be determined.

Discussion Questions

A) Verify that the linear code $C = \langle 11000, 01111, 11110, 01010\rangle$ is cylic, and find the generator polynomial $g(x)$.

B) In general, given a spanning set S for a linear code, how could you determine (in an economical way!) whether the code is cyclic. State and prove a criterion for when this is true. Hint: The cyclic permutation π is a linear mapping.

C) If you know a generator polynomial for a cyclic code C, how can you write down a generator matrix for C *with no extra work*?

D) Since the generator polynomial for a cyclic code of blocklength n must be a divisor of x^n+1, if we know the complete *factorization* of x^n+1 in $K[x]$, then we can determine all the cyclic codes for that n. Verify that

$$x^7+1 = (x+1)(x^6+x^5+x^4+x^3+x^2+x+1) = (x+1)(x^3+x+1)(x^3+x^2+1)$$

Each of the factors in the last product is *irreducible* – it cannot be factored farther into factors of positive degree. Using this information, determine how many cyclic codes of length $n = 7$ there are, and give the generator polynomial and dimension for each.

E) Determine how many cyclic codes of length $n = 12$ there are, and give the generator polynomial and dimension for each. Hint: Look at theorem 4.4.3 and Corollary 4.4.4 in the text.

Assignment

Group writeups due in class on Monday, March 25.