Homework 8
Algebraic Coding Theory
Math 525
Stephen Giang RedID: 823184070

Problem 3:

(a) **Exercise 4.2.8:** Find all words v of length n, such that $\pi(v) = v$.

Notice we need to be able to shift every element and end up with v, so we get v is the vector of all 1's or all 0's.

(b) **Exercise 4.2.9:** Find all words v of length 6, such that $\pi^2(v) = v$.

$$v = 111111, 000000, 101010, 010101$$

And $\pi^3(v) = v$

$$v = 111111, 000000, 000111, 111000$$

Problem 4:

Exercise 4.2.20: For each of the words below, find the generator polynomial for the smallest linear cyclic code containing that word.

(a) 010101

Notice that $g(x) = gcd(x + x^3 + x^5, x^6 + 1) = x^4 + x^2 + 1$

(b) 01100110

Notice that $g(x) = gcd(x + x^2 + x^5 + x^6, x^8 + 1) = x^5 + x^4 + x + 1$

Problem 5:

Exercise 4.2.22: For each of the codes $C = \langle S \rangle$ with S defined below, find the generator polynomial $g(x)$ and then represent each word in the code as a multiple of $g(x)$.

(c) $S = \{0101, 1010, 1100\}$

Notice that all the words are linearly independent. So we get that C is a $(n = 4, k = 3)$ linear-cyclic code. We get the degree of the generator matrix is $t = n - k = 1$. Notice that the third word corresponds to a degree 1 polynomial, such that $g(x) = 1 + x$.

(d) $S = \{1000, 0100, 0010, 0001\}$

Notice that all the words are linearly independent. So we get that C is a $(n = 4, k = 4)$ linear-cyclic code. We get the degree of the generator matrix is $t = n - k = 0$. Notice that the first word corresponds to a degree 0 polynomial, such that $g(x) = 1$.

Problem 6:

(a) **Exercise 4.3.4:** Let $g(x) = 1 + x^2 + x^3$ be the generator polynomial of a linear cyclic code of length 7.

(a) Encode the following message polynomials: $1 + x^3, x, x + x^2 + x^3$

$$\begin{aligned} v &= (1 + x^3)g(x) = x^6 + x^5 + x^2 + 1 \\ v &= xg(x) = x + x^3 + x^4 \\ v &= (x + x^2 + x^3)g(x) = x^6 + x^2 + x \end{aligned}$$

(b) Find the message polynomial corresponding to the codewords $c(x)$: $x^2 + x^4 + x^5, 1 + x + x^2 + x^4, x^2 + x^3 + x^4 + x^6$

$$\begin{aligned} a &= (x^2 + x^4 + x^5)/g(x) = x^2 \\ a &= (1 + x + x^2 + x^4)/g(x) = x + 1 \\ a &= (x^2 + x^3 + x^4 + x^6)/g(x) = x^3 + x^2 \end{aligned}$$

(b) **Exercise 4.3.5:** Find a basis and generating matrix for the linear cyclic code of length n with generator polynomial $g(x)$.

$n = 7, g(x) = 1 + x^2 + x^3$.

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

(c) **Exercise 4.3.6:** Show that the linear code with given generator matrix is cyclic and find the generator polynomial.

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

$g(x) = 1 + x + x^3 + x^4$. Also notice that $r_1 = \pi(r_3)$

Problem 7:

(a) **Exercise 4.3.8:** Find a parity check matrix for the linear cyclic code of length 7 with generator $g(x) = 1 + x + x^2 + x^4$.

Notice the following:

$$\begin{aligned}
1 &\mod g(x) = 1 \\
x &\mod g(x) = x \\
x^2 &\mod g(x) = x^2 \\
x^3 &\mod g(x) = x^3 \\
x^4 &\mod g(x) = 1 + x + x^2 \\
x^5 &\mod g(x) = x^3 + x^2 + x \\
x^6 &\mod g(x) = x^3 + x + 1
\end{aligned}$$

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}$$

Problem 8:

(a) **Exercise 4.4.6:** Find the number of proper linear cyclic codes of length n, where $n = 4$

Notice we can find the number of proper cyclic codes from : $(2^r - 1)^z - 2$.

Notice that $n = 4 = 2^2 * 1$. So $r = 2, s = 1$. Notice that $x^2 + 1$ has 1 irreducible factor such that $z = 1$. Now we get $(4 + 1)^1 - 2 = 3$ proper cyclic codes.

(b) **Exercise 4.4.7:** Find the generator polynomial for all proper linear cyclic codes of length n, where $n = 4$

The generator polynomials of proper linear cyclic codes are factors of $x^4 + 1$ excluding itself and 1. So we get $g(x) = (x + 1), (x + 1)^2, (x + 1)^3$

(c) **Exercise 4.4.8:** Find two generators of degree 4 for a linear cyclic code of length 7.

The generator polynomials for a cyclic code of length 7 are $\left(x^3 + x + 1\right)\left(x^3 + x^2 + 1\right)(x + 1)$. To get the generators of degree 4, we have 2 choices: $(x+1)\left(x^3 + x^2 + 1\right)$ or $(x+1)\left(x^3 + x + 1\right)$

(d) **Exercise 4.4.9:** Find a generator and a generating matrix for a linear code of length n and dimension k where $n = 12, k = 5$.

Notice the generator polynomials: $x^8 + x^4 + 1$ and $x^4 + 1$.

Because $n - k = 7$, we get that $g(x) = x^4 + 1$ such that

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