MAT 148, Winter 2016
Solutions to HW 7

2. Prove that $\mathbb{Z}_2[x]/(x^3-1)$ is not a field by presenting an element with no multiplicative inverse.

Solution: Let $f(x)=x^3-1$. We have $(x-1)(x^2+x+1)=x^3-1=0$ mod $f(x)$. Suppose that $x-1$ is invertible modulo $f(x)$, then

$$x^2+x+1=(x-1)^{-1}(x-1)(x^2+x+1)=(x-1)^{-1}\cdot 0=0,$$

contradiction. Therefore $x-1$ has no multiplicative inverse. Similarly, x^2+x+1 has no multiplicative inverse as well.

9a. Write the generator polynomials and generator matrices for all binary cyclic codes of length 7.

Solution: We have $x^7-1=x^{2^3-1}-1$, so it is divisible by all irreducible polynomials with degrees dividing 3. Therefore:

$$x^7-1=(x+1)(x^3+x+1)(x^3+x^2+1) \mod 2.$$

Therefore we have 6 possible cyclic codes:

$$g(x)=x+1,\ G=\begin{pmatrix}1&1&0&0&0&0&0\\0&1&1&0&0&0&0\\0&0&1&1&0&0&0\\0&0&0&1&1&0&0\\0&0&0&0&1&1&0\\0&0&0&0&0&1&1\end{pmatrix};$$

$$g(x)=x^3+x+1,\ G=\begin{pmatrix}1&0&1&1&0&0&0\\0&1&0&1&1&0&0\\0&0&1&0&1&1&0\\0&0&0&1&0&1&1\end{pmatrix};$$

$$g(x)=x^3+x^2+1,\ G=\begin{pmatrix}1&1&0&1&0&0&0\\0&1&1&0&1&0&0\\0&0&1&1&0&1&0\\0&0&0&1&1&0&1\end{pmatrix};$$

$$g(x) = (x+1)(x^3+x+1) = x^4+x^3+x^2+1,\ G = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix};$$

$$g(x) = (x+1)(x^3+x^2+1) = x^4+x^2+x+1,\ G = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix};$$

$$g(x) = (x^3+x+1)(x^3+x^2+1) = x^6+x^5+x^4+x^3+x^2+x+1,\ G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Remark: In principle, one may consider two more codes with $g_1(x) = 1$or

$$g_2(x) = (x+1)(x^3+x+1)(x^3+x^2+1) = x^7-1 = 0 \mod x^7-1,$$

The cyclic code for g_1 contains all binary sequences of length 7 as codewords, while the cyclic code for g_2 has only 0 as a codeword.

11. Which length 7 binary cyclic codes contain the vector $(0,1,0,0,1,1,1)$?

Solution: This vector represents a polynomial x^5+x^2+x+1, which can be factored as follows:

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

The set of codewords in a cyclic code with generating polynomial $g(x)$ coincides with the set of polynomials mod x^n-1, divisible by $g(x)$. Therefore, all possible $g(x)$ should divide $(x+1)^2(x^3+x+1)$, so

$$g(x) = (x+1),\ g(x) = (x^3+x+1) \text{ or } g(x) = (x+1)(x^3+x+1).$$

The generating matrices for these codes are written above.

13. We know that modulo 2

$$x^{15}1 = (x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1).$$

How many binary cyclic codes of length 15 are there?

Solution: The generating polynomial $g(x)$ for a cyclic code should divide x^15-1, so should be a product of several of the above 5 irreducible factors. Such a product can contain 1,2,3, or 4 factors, so the number of options for $g(x)$ is

$$\binom{5}{1} + \binom{5}{2} + \binom{5}{3} + \binom{5}{4} = 30.$$

Therefore, there are 30 binary cyclic codes of length 15 (or 32, if one includes two trivial codes with $g(x) = 1$ and $g(x) = x^{15}-1$).