Homework 2 : Due by end of class on Tuesday April 5

1. (Weights of codewords in a cyclic code)
   Let $g(X)$ be the generator polynomial of a binary cyclic code of length $n$.
   
   (a) Show that if $g(X)$ has $X + 1$ as a factor then the code contains no codewords of odd weight.
   
   (b) Show that if $n$ is odd and $X + 1$ is not a factor of $g(X)$ then the code contains the codeword consisting of all 1’s.
   
   (c) Show that if $n$ is the smallest integer such that $g(X)$ divides $X^n + 1$ then the code has minimum weight at least 3.
   
   (d) Suppose $g(X)$ is such that the code contains both even-weight and odd-weight codewords. Let $A(z)$ denote the weight enumerator polynomial of the code. Show that the polynomial $(X + 1)g(X)$ also generates a binary cyclic code of length $n$, and that this has weight enumerator polynomial
   \[ A_1(z) = \frac{1}{2} [A(z) + A(-z)] \, . \]

2. (Cyclic codes)
   
   (a) i. Show that $g(X) = 1 + X^2 + X^4 + X^6 + X^7 + X^{10}$ generates a (21,11) cyclic code.
      
      ii. Let $r(X) = 1 + X^5 + X^{17}$ be a received polynomial. Compute the syndrome of $r(X)$.
   
   (b) Let $C_1$ and $C_2$ be two cyclic codes of length $n$ generated by $g_1(x)$ and $g_2(x)$ respectively. What is the generator polynomial for the smallest cyclic code that contains the set $C_1 \cup C_2$?
   
   (c) Let $C_1$ and $C_2$ be two cyclic codes of length $n$ generated by $g_1(x)$ and $g_2(x)$ respectively. Show that the code polynomials common to both $C_1$ and $C_2$ also form a cyclic code $C_3$. Determine the generator polynomial of $C_3$. If $d_1$ and $d_2$ are the minimum distances of $C_1$ and $C_2$ respectively, what can you say about the minimum distance of $C_3$?

3. (Polynomials)
   
   (a) Show that $X^5 + X^3 + 1$ is irreducible over GF(2).
   
   (b) Let $f(X)$ be a polynomial of degree $n$ over GF(2) with nonzero constant term. Let $f^*(X)$ denote its reciprocal polynomial, i.e.
   \[ f^*(X) = X^n f(X^{-1}) \, . \]
   
   i. Prove that $f(X)$ is irreducible over GF(2) if and only if $f^*(X)$ is irreducible over GF(2).
ii. Prove that $f(X)$ is primitive over $\text{GF}(2)$ if and only if $f^*(X)$ is primitive over $\text{GF}(2)$.

4. (*Calculations in finite fields*)

Let $\alpha$ be a primitive element in $\text{GF}(2^4)$ satisfying $\alpha = \alpha^4 + 1$. In the following problems you will find it useful to refer to Table 2.8 on pg. 47 of the text.

(a) Find the roots of $X^3 + \alpha^6 X^2 + \alpha^9 X + \alpha^9$ in $\text{GF}(2^4)$.

(b) Solve the following system of equations in $\text{GF}(2^4)$:

\[
\begin{align*}
X + \alpha^5 Y + Z &= \alpha^7 \\
X + \alpha Y + \alpha^7 Z &= \alpha^9 \\
\alpha^2 X + Y + \alpha^6 Z &= \alpha
\end{align*}
\]

5. (*Determining all binary cyclic codes*)

Determine all the binary cyclic codes of length 21.

*Hint*: What is the factorization of $X^{21} + 1$ into irreducible factors over $\text{GF}(2)$? The decomposition of the nonzero elements of $\text{GF}(64)$ into cyclotomic cosets may be useful in answering this question.