1. (5 points) Consider the set $F = \{a_0 + a_1 X | a_0, a_1 \in \mathbb{F}_2\}$ of polynomials of degree at most 1 with coefficients in $\mathbb{F}_2$. For two polynomials $a(X) = a_0 + a_1 X$ and $b(X) = b_0 + b_1 X$ in F define the addition operator $\oplus$ as
$$a(X) \oplus b(X) = a_0 + b_0 + (a_1 + b_1)X.$$
The addition operator $\oplus$ is just regular polynomial addition. Define the multiplication operator $\otimes$ as
$$a(X) \otimes b(X) = \left[a_0 b_0 + (a_0 b_1 + a_1 b_0)X + a_1 b_1 X^2\right] \bmod (1 + X + X^2).$$
The multiplication operator gives the remainder when $a(X)b(X)$ is divided by $1 + X + X^2$. Show that F is a field with the addition and multiplication operators defined by $\oplus$ and $\otimes$ respectively.

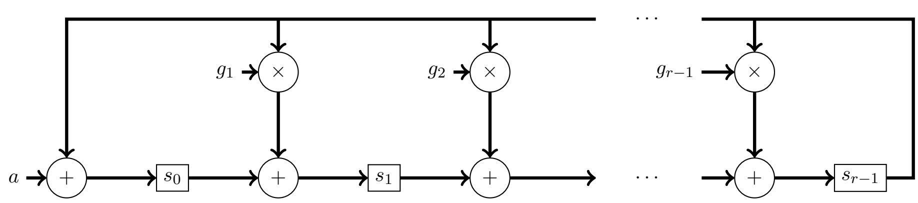
2. (5 points) Let C be an (n, k) binary linear block code having minimum distance d_{min} and weight enumerator $A(z)$. Let $\mathbf{G}$ be a generator matrix of C. Consider the length $3n$ code C_1 with generator matrix $\mathbf{G}_1 = \begin{bmatrix} \mathbf{G} & \mathbf{G} & \mathbf{G} \end{bmatrix}$. Answer the following in terms of the parameters of C. Explain your answers.
   (a) What is the dimension of C_1?
   (b) What is the minimum distance of C_1?
   (c) What is the weight enumerator of C_1?

3. (5 points) Let C be a binary Hamming code of dimension k.
   (a) Find the number of minimum weight nonzero codewords in C in terms of k.
   (b) Find the number of maximum weight codewords in C as a function of k.

4. (5 points) Show that the binary Reed-Muller codes RM$(1, 4)$ and RM$(2, 4)$ are dual codes of each other.

5. (5 points) Consider a (n, k) binary cyclic code C with generator polynomial $g(X)$.
   (a) Show that the polynomial $g^*(X) = X^{n-k} g(X^{-1})$ generates an (n, k) cyclic code.
   (b) Let C_1 be the cyclic code generated by $g^*(X)$. Find the weight enumerator of C_1 in terms of the weight enumerator $A(z)$ of C.

6. (5 points) Let $g(X) = 1 + g_1 X + g_2 X^2 + \cdots + g_{r-1} X^{r-1} + X^r$ be a polynomial whose coefficients define the following circuit where $a, g_i, s_i \in \mathbb{F}_2$. The addition operator corresponds addition in $\mathbb{F}_2$. The rectangular blocks correspond to a shift register where the bits $s_0, s_1, \ldots, s_{r-1}$ represent the current state.



   (a) If $s(X) = s_0 + s_1 X + \cdots + s_{r-1} X^{r-1}$ is the polynomial corresponding to the current state of the circuit before the input a is applied, find the polynomial corresponding to the next state in terms of $s(X)$, $g(X)$ and a.
   (b) Suppose the initial state of the circuit is all-zeros, i.e. $s_i = 0$ for all i. If the input corresponds to a sequence of n bits $a_{n-1}, a_{n-2}, \ldots, a_1, a_0$ with the shift register being shifted right once after each input bit is applied, show that the polynomial corresponding to the final state is the remainder when $\sum_{i=0}^{n-1} a_i X^i$ is divided by $g(X)$.