PROBLEMS

5.1 Consider the (15, 11) cyclic Hamming code generated by $\mathbf{g}(X) = 1 + X + X^4$.
  a. Determine the parity polynomial $\mathbf{h}(X)$ of this code.
  b. Determine the generator polynomial of its dual code.
  c. Find the generator and parity matrices in systematic form for this code.

5.2 Devise an encoder and a decoder for the (15, 11) cyclic Hamming code generated by $\mathbf{g}(X) = 1 + X + X^4$.

5.3 Show that $\mathbf{g}(X) = 1 + X^2 + X^4 + X^6 + X^7 + X^{10}$ generates a (21, 11) cyclic code. Devise a syndrome computation circuit for this code. Let $\mathbf{r}(X) = 1 + X^5 + X^{17}$ be a received polynomial. Compute the syndrome of $\mathbf{r}(X)$. Display the contents of the syndrome register after each digit of $\mathbf{r}$ has been shifted into the syndrome computation circuit.

5.4 Shorten this (15, 11) cyclic Hamming by deleting the seven leading high-order message digits. The resultant code is an (8, 4) shortened cyclic code. Design a decoder for this code that eliminates the extra shifts of the syndrome register.

5.5 Shorten the (31, 26) cyclic Hamming code by deleting the 11 leading high-order message digits. The resultant code is a (20, 15) shortened cyclic code. Devise a decoding circuit for this code that requires no extra shifts of the syndrome register.

5.6 Let $\mathbf{g}(X)$ be the generator polynomial of a binary cyclic code of length n.
  a. Show that if $\mathbf{g}(X)$ has $X + 1$ as a factor, the code contains no codewords of odd weight.
  b. If n is odd and $X + 1$ is not a factor of $\mathbf{g}(X)$, show that the code contains a codeword consisting of all 1's.
  c. Show that the code has a minimum weight of at least 3 if n is the smallest integer such that $\mathbf{g}(X)$ divides $X^n + 1$.

5.7 Consider a binary (n, k) cyclic code C generated by $\mathbf{g}(X)$. Let

$$\mathbf{g}^*(X) = X^{n-k}\mathbf{g}(X^{-1})$$

be the reciprocal polynomial of $\mathbf{g}(X)$.
  a. Show that $\mathbf{g}^*(X)$ also generates an (n, k) cyclic code.
  b. Let C^* denote the cyclic code generated by $\mathbf{g}^*(X)$. Show that C and C^* have the same weight distribution.

(*Hint:* Show that

$$\mathbf{v}(X) = v_0 + v_1X + \cdots + v_{n-2}X^{n-2} + v_{n-1}X^{n-1}$$

is a code polynomial in C if and only if

$$X^{n-1}\mathbf{v}(X^{-1}) = v_{n-1} + v_{n-2}X + \cdots + v_1X^{n-2} + v_0X^{n-1}$$

is a code polynomial in C^*.)

5.8 Consider a cyclic code C of length n that consists of both odd-weight and even-weight codewords. Let $\mathbf{g}(X)$ and $A(z)$ be the generator polynomial and weight enumerator for this code. Show that the cyclic code generated by $(X + 1)\mathbf{g}(X)$ has weight enumerator

$$A_1(z) = \tfrac{1}{2}[A(z) + A(-z)].$$

5.9 Suppose that the (15, 10) cyclic Hamming code of minimum distance 4 is used for error detection over a BSC with transition probability $p = 10^{-2}$. Compute the probability of an undetected error, $P_u(E)$, for this code.

5.10 Consider the $(2^m - 1, 2^m - m - 2)$ cyclic Hamming code C generated by $\mathbf{g}(X) = (X + 1)\mathbf{p}(X)$, where $\mathbf{p}(X)$ is a primitive polynomial of degree m. An error pattern of the form

$$\mathbf{e}(X) = X^i + X^{i+1}$$

is called a ***double-adjacent-error pattern***. **Show that no two double-adjacent-error patterns can be in the same coset of a standard array for C. Therefore, the code is capable of correcting all the single-error patterns and all the double-adjacent-error patterns.**

5.11 Devise a decoding circuit for the (7, 3) Hamming code generated by $\mathbf{g}(X) = (X + 1)(X^3 + X + 1)$. The decoding circuit corrects all the single-error patterns and all the double-adjacent-error patterns (see Problem 5.10).

5.12 For a cyclic code, if an error pattern $\mathbf{e}(X)$ is detectable, show that its ith cyclic shift $e^{(i)}(X)$ is also detectable.

5.13 In the decoding of an (n, k) cyclic code, suppose that the received polynomial $\mathbf{r}(X)$ is shifted into the syndrome register from the right end, as shown in Figure 5.11. Show that when a received digit r_i is detected in error and is corrected, the effect of error digit e_i on the syndrome can be removed by feeding e_i into the syndrome register from the right end, as shown in Figure 5.11.

5.14 Let $\mathbf{v}(X)$ be a code polynomial in a cyclic code of length n. Let l be the smallest integer such that

$$\mathbf{v}^{(l)}(X) = \mathbf{v}(X).$$

Show that if $l \neq 0$, l is a factor of n.