بسم تعالی

حل تکلیف شماره ۴ کدگذاری کانال

1– (a) A polynomial over GF(2) with odd number of terms is not divisible by $X + 1$, hence it can not be divisible by $\mathbf{g}(X)$ if $\mathbf{g}(X)$ has $(X+1)$ as a factor. Therefore, the code contains no code vectors of odd weight.

(b) The polynomial $X^n + 1$ can be factored as follows:

$$X^n + 1 = (X+1)(X^{n-1} + X^{n-2} + \cdots + X + 1)$$

Since $\mathbf{g}(X)$ divides $X^n + 1$ and since $\mathbf{g}(X)$ does not have $X + 1$ as a factor, $\mathbf{g}(X)$ must divide the polynomial $X^{n-1} + X^{n-2} + \cdots + X + 1$. Therefore $1 + X + \cdots + X^{n-2} + X^{n-1}$ is a code polynomial, the corresponding code vector consists of all $1'$s.

(c) First, we note that no X^i is divisible by $\mathbf{g}(X)$. Hence, no code word with weight one. Now, suppose that there is a code word $\mathbf{v}(X)$ of weight 2. This code word must be of the form,

$$\mathbf{v}(X) = X^i + X^j$$

with $0 \le i < j < n$. Put $\mathbf{v}(X)$ into the following form:

$$\mathbf{v}(X) = X^i(1 + X^{j-i}).$$

Note that $\mathbf{g}(X)$ and X^i are relatively prime. Since $\mathbf{v}(X)$ is a code word, it must be divisible by $\mathbf{g}(X)$. Since $\mathbf{g}(X)$ and X^i are relatively prime, $\mathbf{g}(X)$ must divide the polynomial $X^{j-i} + 1$. However, $j - i < n$. This contradicts the fact that n is the smallest integer such that $\mathbf{g}(X)$ divides $X^n + 1$. Hence our hypothesis that there exists a code vector of weight 2 is invalid. Therefore, the code has a minimum weight at least 3.

2– (a) Note that $X^n + 1 = \mathbf{g}(X)\mathbf{h}(X)$. Then

$$X^n(X^{-n} + 1) = X^n\mathbf{g}(X^{-1})\mathbf{h}(X^{-1})$$

$$1 + X^n = \left[X^{n-k}\mathbf{g}(X^{-1})\right]\left[X^k\mathbf{h}(X^{-1})\right]$$
$$= \mathbf{g}^*(X)\mathbf{h}^*(X).$$

where $\mathbf{h}^*(X)$ is the reciprocal of $\mathbf{h}(X)$. We see that $\mathbf{g}^*(X)$ is factor of $X^n + 1$. Therefore, $\mathbf{g}^*(X)$ generates an (n, k) cyclic code.

(b) Let C and C^* be two (n, k) cyclic codes generated by $\mathbf{g}(X)$ and $\mathbf{g}^*(X)$ respectively. Let $\mathbf{v}(X) = v_0 + v_1X + \cdots + v_{n-1}X^{n-1}$ be a code polynomial in C. Then $\mathbf{v}(X)$ must be a multiple of $\mathbf{g}(X)$, i.e.,

$$\mathbf{v}(X) = \mathbf{a}(X)\mathbf{g}(X).$$

Replacing X by X^{-1} and multiplying both sides of above equality by X^{n-1}, we obtain

$$X^{n-1}\mathbf{v}(X^{-1}) = \left[X^{k-1}\mathbf{a}(X^{-1})\right]\left[X^{n-k}\mathbf{g}(X^{-1})\right]$$

Note that $X^{n-1}\mathbf{v}(X^{-1})$, $X^{k-1}\mathbf{a}(X^{-1})$ and $X^{n-k}\mathbf{g}(X^{-1})$ are simply the reciprocals of $\mathbf{v}(X)$, $\mathbf{a}(X)$ and $\mathbf{g}(X)$ respectively. Thus,

$$\mathbf{v}^*(X) = \mathbf{a}^*(X)\mathbf{g}^*(X). \tag{1}$$

From (1), we see that the reciprocal $\mathbf{v}^*(X)$ of a code polynomial in C is a code polynomial in C^*. Similarly, we can show the reciprocal of a code polynomial in C^* is a code polynomial in C. Since $\mathbf{v}^*(X)$ and $\mathbf{v}(X)$ have the same weight, C^* and C have the same weight distribution.

3–

Let C_1 be the cyclic code generated by $(X + 1)\mathbf{g}(X)$. We know that C_1 is a subcode of C and C_1 consists all the even-weight code vectors of C as all its code vectors. Thus the weight enumerator $A_1(z)$ of C_1 should consists of only the even-power terms of $A(z) = \sum_{i=0}^{n} A_i z^i$. Hence

$$A_1(z) = \sum_{j=0}^{\lfloor n/2 \rfloor} A_{2j} z^{2j} \tag{1}$$

Consider the sum

$$A(z) + A(-z) = \sum_{i=0}^{n} A_i z^i + \sum_{i=0}^{n} A_i(-z)^i$$

$$= \sum_{i=0}^{n} A_i \left[z^i + (-z)^i \right].$$

We see that $z^i + (-z)^i = 0$ if i is odd and that $z^i + (-z)^i = 2z^i$ if i is even. Hence

$$A(z) + A(-z) = \sum_{j=0}^{\lfloor n/2 \rfloor} 2A_{2j} z^{2j} \tag{2}$$

From (1) and (2), we obtain

$$A_1(z) = 1/2 \left[A(z) + A(-z) \right].$$

4– Let $\mathbf{e}_1(X) = X^i + X^{i+1}$ and $\mathbf{e}_2(X) = X^j + X^{j+1}$ be two different double-adjacent-error patterns such that $i < j$. Suppose that $\mathbf{e}_1(X)$ and $\mathbf{e}_2(X)$ are in the same coset. Then $\mathbf{e}_1(X) + \mathbf{e}_2(X)$ should be a code polynomial and is divisible by $\mathbf{g}(X) = (X+1)\mathbf{p}(X)$. Note that

$$\mathbf{e}_1(X) + \mathbf{e}_2(X) = X^i(X+1) + X^j(X+1)$$

$$= (X+1)X^i(X^{j-i} + 1)$$

Since $\mathbf{g}(X)$ divides $\mathbf{e}_1(X) + \mathbf{e}_2(X)$, $\mathbf{p}(X)$ should divide $X^i(X^{j-i} + 1)$. However $\mathbf{p}(X)$ and X^i are relatively prime. Therefore $\mathbf{p}(X)$ must divide $X^{j-i} + 1$. This is not possible since $j - i < 2^m - 1$ and $\mathbf{p}(X)$ is a primitive polynomial of degree m (the smallest integer n such that $\mathbf{p}(X)$ divides $X^n + 1$ is $2^m - 1$). Thus $\mathbf{e}_1(X) + \mathbf{e}_2(X)$ can not be in the same coset.

5– Note that $\mathbf{e}^{(i)}(X)$ is the remainder resulting from dividing $X^i\mathbf{e}(X)$ by $X^n + 1$. Thus

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

Note that $\mathbf{g}(X)$ divides $X^n + 1$, and $\mathbf{g}(X)$ and X^i are relatively prime. From (1), we see that if $\mathbf{e}(X)$ is not divisible by $\mathbf{g}(X)$, then $\mathbf{e}^{(i)}(X)$ is not divisible by $\mathbf{g}(X)$. Therefore, if $\mathbf{e}(X)$ is detectable, $\mathbf{e}^{(i)}(X)$ is also detectable.

6–

(a) Any error pattern of double errors must be of the form,

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

where $j > i$. If the two errors are not confined to $n - k = 10$ consecutive positions, we must have

$$j - i + 1 > 10,$$

$$15 - (j - i) + 1 > 10.$$

Simplifying the above inequalities, we obtain

$$j - i > 9$$

$$j - i < 6.$$

This is impossible. Therefore any double errors are confined to 10 consecutive positions and can be trapped.

(b) An error pattern of triple errors must be of the form,

$$\mathbf{e}(X) = X^i + X^j + X^k,$$

where $0 \leq i < j < k \leq 14$. If these three errors can not be trapped, we must have

$$k - i > 9$$

$$j - i < 6$$

$$k - j < 6.$$

If we fix i, the only solutions for j and k are $j = 5 + i$ and $k = 10 + i$. Hence, for three errors not confined to 10 consecutive positions, the error pattern must be of the following form

$$\mathbf{e}(X) = X^i + X^{5+i} + X^{10+i}$$

for $0 \leq i < 5$. Therefore, only 5 error patterns of triple errors can not be trapped.