ECC HW3

2021年10月17日 上午 03:24

90

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

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

The cyclic code generated by $(X+1)g(X)$ is a subcode of C that contains all even weight codewords.

Therefore, if we define $A(z) = \sum_{i=0}^{n} A_i z^i$,

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

$$\Rightarrow \frac{1}{2}[A(z) + A(-z)]$$

$$= \frac{1}{2}\left[\sum_{i=0}^{n} A_i z^i + \sum_{i=0}^{n} A_i z^i (-1)^i\right]$$

$$= \frac{1}{2}\left(\sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} A_{2j} z^{2j}\right) \times 2 = \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} A_{2j} z^{2j} = A_1(z) \#$$

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.

Suppose $e_1(X) = X^i + X^{i+1}$ & $e_2(X) = X^j + X^{j+1}$ $(i<j)$ are in the same coset, then there exists a code poly. $u(X)$ s.t. $e_1(X) = e_2(X) + u(X) \Rightarrow e_1(X) + e_2(X) = u(X)$

Also, since $u(X)$ is a code polynomial, we have

$u(X) = Q(X)\,[(X+1)\,p(X)]$

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

Since $p(X)$ & X^i are relatively prime,

$p(X) \mid (1+X^{j-i})$ where $j-i < 2^m-1$ ($\because n = 2^m-1$)

However the smallest integer 'l' such that

$p(X) \mid (X^l+1)$ is 2^m-1 due to the property

of primitive poly. $\rightarrow\leftarrow$

Therefore, there exists no $e_1(X)$ and $e_2(X)$ in

the same coset ✗

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.

Suppose $n = ql + r$, $0 \le r < l$

$V(X) = V^{(n)}(X) = V^{(ql+r)}(X) = V^{(r)}(X)$

However, l is the smallest integer s.t. $V^{(l)}(X) = V(X)$

Therefore, $r = 0$, namely l is a factor of n ✗

5.15 Let $\mathbf{g}(X)$ be the generator polynomial of an (n, k) cyclic code C. Suppose C is interleaved to a depth of λ. Prove that the interleaved code C^λ is also cyclic and its generator polynomial is $\mathbf{g}(X^\lambda)$.

We define the message polynomial of the i^{th} interleaved code as $u_i(X)$ where $0 \le i < \lambda$, and the corresponding code polynomial is $V_i(X) = u_i(X)g(X)$.

Then, for code polynomial $v(X)$ of the interleaved code, we have:

$$v(X) = \sum_{i=0}^{\lambda-1} v_i(X^\lambda) X^i = \sum_{i=0}^{\lambda-1} u_i(X^\lambda) g(X^\lambda) X^i$$

$$= g(X^\lambda) \left[\sum_{i=0}^{\lambda-1} u_i(X^\lambda) X^i \right]$$

Also, degree of $g(X^\lambda)$ is λr, which implies that $g(X^\lambda)$ is the generator polynomial of the interleaved code #

5.16 Construct all the binary cyclic codes of length 15. (*Hint:* Using the fact that $X^{15}+1$ has all the nonzero elements of $GF(2^4)$ as roots and using Table 2.9, factor $X^{15}+1$ as a product of irreducible polynomials.)

From Table 2.9 we have:

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

Each polynomial generate a cyclic codes, where

$$\begin{cases} (X+1) & \text{generates a } (15,14) \text{ code} \\ (X^4+X+1) & \text{" } (15,11) \text{ "} \\ (X^4+X^3+X^2+X+1) & \text{" } (15,11) \text{ "} \\ (X^2+X+1) & \text{" } (15,13) \text{ "} \\ (X^4+X^3+1) & \text{" } (15,11) \text{ "} \end{cases}$$

#