ECC Midterm

2021年10月17日　　上午 03:24

1. (a) (5%) Determine whether X^4+1 is irreducible over $GF(2)$ or not.
   (b) (5%) Determine whether $X^5+X^4+X^2+X+1$ is irreducible over $GF(2)$ or not.
   (c) (5%) Let α be a primitive element of $GF(16)$ with $1+\alpha+\alpha^4=0$. Determine whether X^2+X+1 is irreducible over $GF(4)$ or not. $\alpha^{15}=1$ ~~$1, \alpha, \alpha^2, \alpha^3$~~

(a) Check all polynomial with degree lower than or equal to $\lfloor \frac{4}{2} \rfloor = 2$, This includes

$X^2+X+1,\ \cancel{X^2+1},\ X+1,\ X$

$X^4+1 = (X^2+X+1)(X^2+X)+(X+1)$

$X^4+1 = (X^2+1)(X^2+1) \Rightarrow$ is reducible

(b) $X^5+X^4+X^2+X+1 = f(X)$

$f(X) = (X^2+X+1)(X^3+X)+1$

$f(X) = (X^2+1)(X^3+X^2+X)+1 \quad \Rightarrow$ is irreducible

$f(X) = (X+1)(X^4+X)+1$

$f(X) = X(X^4+X^3+X+1)+1$

(c) $\alpha^{15}=1,\ \alpha^4+\alpha+1=0$? Ch-1, P.11

X^2+X+1 is reducible over $GF(4)$?

$\alpha^5 \quad \alpha^{10}$

$0, 1, \alpha, \alpha^{-1}$ $\qquad X, X+1, X+\alpha, X+\alpha^{-1}$

$X^2+X+1 = X(X+1)+1$

$X^2+X+1 = (X+\alpha)(X+\alpha^{-1})$ $\quad \therefore$ it is reducible.

$\gamma^{63} = 1$

2. Consider a primitive element of the finite field $GF(2^6)$ for which $1 + \alpha + \alpha^6 = 0$.
(a) (5%) Find all the field elements of $GF(2^6)$ of order 9.
(b) (5%) Express α^{13} in polynomial form.
(b) (5%) Find the binary minimal polynomial of α^{21}.

$\beta^9 = 1$

(b) $\alpha^{13} = (\alpha^6)^2 \alpha = (1+\alpha)^2 \alpha$

$= (\alpha^2+1)\alpha = \alpha^3 + \alpha$

(a) $\alpha^7, 14, 28, 56, \cancel{4}49, 35$

β order $= 9$

$\Rightarrow \beta^9 = 1$

$112 - 63 = 49$ $\quad$ $98 - 63 = 35$ $\quad$ 112

(c) min deg. $f(X)$ s.t. $f(\alpha^{21}) = 0$

$1, 2, 4, 8, 16, 32$

$3, \ldots$

$5, \ldots$

$7, 14, 28, 56, 49, 35$

$21, 42, \times$

$(X+\alpha^{21})(X+\alpha^{42}) = X^2 + X + 1$

$2^8 = 128$

3. Let α a primitive element in $GF(2^8)$.
(a) (5%) Show all the conjugates of α over $GF(2)$.
(b) (5%) Find an element in $GF(2^8)$ which is a primitive $17th$ root of unity.

$255 = 17 \times 15$ $\qquad \beta^{17} = 1$

(a) $\alpha^{1,2,4,8,16,32,64}$

(b) $\beta^{17} = 1$, $\beta = \alpha^{15}$

4. (a) (5%) Let $g(X) = 1 + X + X^4$ be the generator polynomial of an $(15, 11)$ binary cyclic code C. Find a generator matrix of C.
(b) (5%) Find a parity check matrix of C.
(c) (5%) Use $g(X)$ to systematically encode the message $u(X) = 1+X^3$ into a codeword of C.

(a)

$$11 \left[\begin{array}{ccccccccccccccc}
1 & 1 & 0 & 0 & 1 & & & & & & & & & & \\
 & 1 & 1 & 0 & 0 & 1 & & & & & & & \mathbf{0} & & \\
 & & 1 & 1 & 0 & 0 & 1 & & & & & & & & \\
 & & & 1 & 1 & 0 & 0 & 1 & & & & & & & \\
 & & & & 1 & 1 & 0 & 0 & 1 & & & & & & \\
 & & & & & 1 & 1 & 0 & 0 & 1 & & & & & \\
 & & & & & & 1 & 1 & 0 & 0 & 1 & & & & \\
 & & \mathbf{0} & & & & & 1 & 1 & 0 & 0 & 1 & & & \\
 & & & & & & & & 1 & 1 & 0 & 0 & 1 & & \\
 & & & & & & & & & 1 & 1 & 0 & 0 & 1 & \\
 & & & & & & & & & & 1 & 1 & 0 & 0 & 1
\end{array}\right]$$

15

(b) $h(x)\,\cancel{g(x)} = x^{15}+1$ $\quad g(x) \to 1+x+x^4$

$x^{11}h(x^{-1})$

$h(x) = x^{11}+x^8+x^7+x^5+x^3+x^2+x+1$

$x^{11}h(x^{-1}) = x^{11}+x^{10}+x^9+x^8+x^6+x^4+x^3+1$

$$
4\left[\begin{array}{ccccccccccccccc}
1&1&1&1&0&1&0&1&1&0&0&1&&&0\\
&1&1&1&1&0&1&0&1&1&0&0&1&&\\
&&1&1&1&1&0&1&0&1&1&0&0&1&\\
0&&&1&1&1&1&0&1&0&1&1&0&0&1
\end{array}\right]
$$
$\underbrace{\qquad\qquad\qquad\qquad\qquad}_{15}$

(c) $u(x) = 1+x^3$

$x^4u(x) = x^7+x^4$

$x^7+x^4 = (x^4+x+1)\,x^3+x^3$

$\Rightarrow x^7+x^4+x^3$

$(0\,0\,0\,1\,1\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0)$

5. Consider an (n, k) linear code C whose generator matrix G contains no zero column. Arrange all the codewords of C as rows of a 2^k-by-n array.
(a) (5%) Show that no columns of the array contains only zeros.
(b) (5%) Show that each column of the array consists of 2^{k-1} zeros and 2^{k-1} ones.

6. (7%) Let $\mathbf{v}(X)$ be a 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.

7. (10%) Prove that the $(m-r-1)$th-order RM code, RM$(m-r-1, m)$ is the dual code of the rth order RM code, RM(r, m).

8. (8%) Let $g(X)$ 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 $g(X^{\lambda})$.

9. (a) (5%) Describe the procedure of syndrome decoding for an (n, k) binary cyclic code C.
(b) (5%) Show that for this cyclic code C all the polynomials in the same coset have the same syndrome.

(a) ① get $\bar{r}$ $\Rightarrow$ $\bar{S} = \bar{r} H^T$

② $\bar{s} = \bar{r} H^T = (\bar{v} + \bar{e}) H^T = \bar{e} H^T$

$\bar{e}$ will have 2^k solutions but the most likely one $\Rightarrow$ chosen

Usually, we record a LUT will size 2^{n-k} where each map to its coset leader