Review Week 10: Cyclic codes (worked example of classification). Golay codes. Classification of perfect codes

2022-11-28

Reminder: online test worth 10% of the final mark

The coursework test will open tomorrow 29-Nov at 11am. Please practise doing the Mock Test.

Working with cyclic codes in $\mathbb{F}_q^n$

- **Cyclic codes in** $\mathbb{F}_q^n \leftrightarrow$ **monic polynomial factors of** $\boxed{x^n - 1}$ **in** $\boxed{\mathbb{F}_q[x]}$
- **The first step is to factorise** $x^n - 1$ **into irreducible monic factors**
- **If** $n \leq 3$ **and** q **is a small prime, this can always be done manually**
    - **Example: factorise** $x^3 - 1$

over $\mathbb{F}_2$ over $\mathbb{F}_3$

$$\underbrace{(x^n - 1)}_{} = (x-1)\underbrace{(x^{n-1} + x^{n-2} + \dots + x + 1)}_{}$$

compare with $\frac{q^n - 1}{q - 1} = q^{n-1} + q^{n-2} + \dots + q + 1$

$$x^3 - 1 = (x-1)(x^2 + x + 1)$$

x^2+x+1

$= (x-1)(x-1)$ over $\mathbb{F}^3$

$1 = (-1)(-1)$

$\boxed{\text{Over } \mathbb{F}_3}$

x^2+x+1 is not irreducible

iff $x^2+x+1 = (x-a)(x-b)$

a, b roots of x^2+x+1

$\mathbb{F}_3$: $x^3 - 1 = (x-1)^3 = (x+2)^3$

$(x-1)^3 = x^3 - 3x^2 + 3x - 1$
$= x^3 - 1 = x^3 + 2$

Substitute 0: $0^2 + 0 + 1 \neq 0$

Substitute 1: $1^2 + 1 + 1 = 0$

Over $\mathbb{F}_2$: $x^3 - 1 = (x-1)(x^2+x+1) = (x+1)(x^2+x+1)$

x^2+x+1 has no roots in $\mathbb{F}_2$

$0^2 + 0 + 1 \neq 0$, $1^2 + 1 + 1 \neq 0$

and so x^2+x+1 is irreducible.

- If $n > 3$, this may require algorithms beyond the scope of this course

Worked example: $\mathbb{F}_2^7$

Given that $x^3 + x + 1$ is an irreducible factor of $x^7 - 1$ in $\mathbb{F}_2[x]$, write down all cyclic codes in $\mathbb{F}_2^7$.

$$x^7 - 1 = (x+1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) \quad (*)$$

$$\begin{array}{r|l} & x^3 + x^2 + 1 \\ \hline x^3+x+1 & x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\ - & x^6 + x^4 + x^3 \\ \hline & x^5 + x^2 + x + 1 \\ - & x^5 + x^3 + x^2 \\ \hline & x^3 + x + 1 \\ & x^3 + x + 1 \\ \hline & 0 \end{array}$$

$$\boxed{(*) = (x+1)(x^3+x+1)(x^3+x^2+1)}$$

Possible $g(x)$ (generator polynomials): 8 possibilities.

$g(x) = 1$ $\quad$ $\deg g = 0$ $\quad$ $\dim C = n - \deg g = 7$

$C \leq \mathbb{F}_2^7$ trivial code

$G = I_7$, $\quad d = 1$,

(zero rows) $H = [\quad]$

$g(x) = x + 1$ $\qquad h(x) = \dfrac{x^n - 1}{g(x)} = \dfrac{x^7+1}{x+1} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

$\dim C = 6$

$d = 2$

$$H = [1 \; 1 \; 1 \; 1 \; 1 \; 1 \; 1]$$

$$E_7 = C = \{(x_1, \dots, x_7) : x_1 + x_2 + \dots + x_7 = 0\}$$

$g(x) = x^3 + x + 1$

$\dim C = 7 - 3 = 4$

$$H = \begin{array}{c} \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \\ \begin{matrix} 1 & \;2 & \;5 & \;3 & \;7 & \;6 & \;4 \end{matrix} \end{array} \qquad Ham(3,2) = C$$

$\dim C = 3$

$$h(x) = \frac{x^7+1}{x^3+x+1} = (x+1)(x^3+x^2+1) = \underline{x^4 + x^2 + x + 1}$$

$g = x^3 + x^2 + 1$ another Hamming code $\mathrm{Ham}(3,2)$

$d = 3$ $\dim = 4$ perfect.

$\tilde{g}(x) = (x+1)(x^3+x+1) = x^4 + x^3 + x^2 + 1$

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

This is $C = \mathrm{Ham}(3,2)^{\perp} = \Sigma(3,2)$

$\dim = 3$ $d = 4 = 2^{3-1}$

$g(x) = (x+1)(x^3+x^2+1)$ $\Sigma(3,2)$

$g(x) = (x^3+x+1)(x^3+x^2+1) = x^6+x^5+x^4+x^3+x^2+x+1$

$\longrightarrow G = [\,1\ 1\ 1\ 1\ 1\ 1\ 1\,]$

$C = \mathrm{Rep}(7, \mathbb{F}_2)$

The 8th possibility is $g(x) = x^7 - 1$

Convention: $C = \{0000000\} =$ null code

$\dim C = 0$

$d(C)$ is undefined