

Practice suw

$$x^{15} + 1 = (1+x)(1+x+x^2)(1+x+x^4)(1+x^3+x^4)(1+x+x^2+x^3+x^4) / GF(2)$$

① \exists mã vòng tuyến tính $\mathcal{E}(15, 8)$??

② Với mã được chọn ở trên, xác định ký 2 gby

③ xđ ma trận G & ma trận H

④ Với mã trên, $r(x) = 1+x+x^{10}+x^{12}+x^{14}$ có phải là đa thức mã hay không?

⑤ Nêu các cách (có thể) để tìm phân cho mã

① ~~Giả sử~~ gby là đa thức sinh của $\mathcal{E}(15, 8)$

$$\exists \text{ mã vòng tuyến tính } \mathcal{E}(15, 8) \Leftrightarrow \exists g(x) \Leftrightarrow \begin{cases} g(x) \text{ monic} \\ \deg(g(x)) = 7 \\ x^{15} + 1 \vdots g(x) \end{cases}$$

$$\text{Giả sử } g(x) = (1+x)(1+x+x^2)(1+x+x^4)$$

$$g(x) \begin{cases} \text{monic} \checkmark \\ \deg(g(x)) = 7 \checkmark \\ x^{15} + 1 \vdots g(x) \end{cases}$$

$$\Rightarrow \exists \text{ mã vòng tuyến tính } \mathcal{E}(15, 8)$$

$$\text{Trường hợp: } g(x) \text{ có thể là } (1+x)(1+x+x^2)(1+x+x^4) \\ \text{hoặc } (1+x)(1+x+x^2)(1+x+x^2+x^3+x^4)$$

~~Q1~~

② $\{15, 8\}$, $x^{15} + 1 = (1+x)(1+x+x^2)(1+x+x^4)(1+x^3+x^4)(1+x+x^2+x^3+x^4)$

STT	$g(x)$	$h(x)$
1	$(1+x)(1+x+x^2)(1+x+x^4)$	$h(x) = \frac{x^{15}+1}{g(x)} = (1+x^3+x^4)(1+x+x^2+x^3+x^4)$
2	$g(x) = (1+x)(1+x+x^2)(1+x^3+x^4)$	$h(x) = (1+x+x^4)(1+x+x^2+x^3+x^4)$
3	$g(x) = (1+x)(1+x+x^2)(1+x+x^2+x^3+x^4)$	$h(x) = (1+x+x^4)(1+x^3+x^4)$

③ $g(x) = (1+x)(1+x+x^2)(1+x+x^4) = 1+x+x^3+x^7$

$\Rightarrow \underline{g_0=0, g_1=1, g_2=0, g_3=0}$

$\Rightarrow \begin{cases} g_0 = g_1 = g_3 = g_7 = 1 \\ g_2 = g_4 = g_5 = g_6 = 0 \end{cases}$

$$G_{[8 \times 15]} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$h(x) = (1+x^3+x^4)(1+x+x^2+x^3+x^4) = 1+x+x^2+x^4$$

$\Rightarrow \begin{cases} h_0 = h_1 = h_2 = h_4 = 1 \\ h_3 = h_5 = h_6 = h_7 = 0 \end{cases}$

$$H_{[7 \times 15]} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

④ $r(x)$ là đa thức mã $\Leftrightarrow s(x) \div g(x)$

Ph: $g(x) = (1+x)(1+x+x^2)(1+x+x^4)$
 $= 1+x+x^3+x^7$

~~sis~~

$$\begin{array}{r} 1+x+x^{10}+x^{12}+x^{14} \\ \underline{x^7+x^3+x^7} \\ x^2+x^4 \\ \underline{x^2+x^3} \\ x^3 \end{array} \quad \begin{array}{r} 1+x+x^3+x^7 \\ \underline{x^7+x^3+x^7} \\ 1 \end{array}$$

$s(x) \% g(x) = x +$

$$\begin{array}{r} 1+x+x^{10}+x^{12}+x^{14} \\ \underline{x^7+x^3+x^7} \\ x^2+x^4 \\ \underline{x^2+x^3} \\ x^3 \end{array} \quad \begin{array}{r} 1+x+x^3+x^7 \\ \underline{x^7+x^3+x^7} \\ x^3+x^5+1 \end{array}$$

$\Rightarrow s(x)$ không phải đa thức mã

Ph2: $g(x) = (1+x)(1+x+x^2)(1+x+x^9)$
 $= (1+x+x^3+x^2+x^3)(1+x+x^9)$
 $= (1+x^3)(1+x+x^9)$
 $= 1+x+x^3+x^7+x^9+x^{12}+x^{12}$
 $= 1+x+x^3+x^7$

(1) $r(x)$ là đa thức mà $\Rightarrow r(x) : g(x)$
 $\Rightarrow r(x) / g(x) \Rightarrow 0$

$$\text{TH1: } g(x) = (1+x)(1+x+x^2)(1+x+x^2+x^3+x^4)$$

$$= \frac{1+x^5+x^6}{1+x^3+x^4}$$

$$r(x) \% g(x) = x^3 + x^5 + x^6$$

$\Rightarrow r(x) / g(x) \Rightarrow r(x)$ không phải đa thức mà (1)

$$\text{TH2: } g(x) = (1+x)(1+x+x^2)(1+x^3+x^4)$$

$$= (1+x^3)(1+x^3+x^4)$$

$$= (1+x^3+x^4+x^6+x^7+x^7)$$

$$= 1+x^3+x^4+x^6+x^7$$

$$\begin{array}{r} 1+x^3+x^4+x^6+x^7 \\ x^3+x^4+x^6+x^7 \\ \hline x^3+x^4 \\ x^5+x^6 \\ x^2+x^3 \end{array}$$

$$\begin{array}{r} 1+x^3+x^4+x^6+x^7 \\ x^3+x^4+x^6+x^7 \\ \hline 1 \end{array}$$

$$r(x) \% g(x) = 1+x^2 \Rightarrow r(x) / g(x) \quad (2)$$

$$\text{TH3: } g(x) = (1+x)(1+x+x^2)(1+x+x^2+x^3+x^4)$$

$$= (1+x^3)(1+x+x^2+x^3+x^4)$$

$$= 1+x+x^2+x^3+x^4+x^4+x^5+x^6+x^7$$

$$= 1+x+x^2+x^3+x^4+x^5+x^6+x^7$$

$$\begin{array}{r} 1+x+x^2+x^3+x^4+x^5+x^6+x^7 \\ x^3+x^4+x^5+x^6+x^7 \\ \hline 1+x+x^2+x^3+x^4 \end{array}$$

$$\begin{array}{r} 1+x+x^2+x^3+x^4+x^5+x^6+x^7 \\ x^3+x^4+x^5+x^6+x^7 \\ \hline 1+x+x^2 \end{array}$$

$$\Rightarrow r(x) / g(x) \quad (3)$$

(1), (2), (3) $\Rightarrow r(x)$ không phải đa thức mà