Comm Coding HW 1 CH2 #10, 12, 13, 14, 19

1

#10. $m=5 \rightarrow x^{2^m-1}+1 = x^{31}+1$

$$x^{26}+x^{24}+x^{22}+x^{21}+x^{20}+x^{18}+x^{17}+x^{13}+x^{12}+x^{11}$$

$$x^5+x^3+1 \;\overline{)\; x^{31}+1}$$

$$\underline{x^{31}+x^{29}+x^{26}}$$

$$x^{29}+x^{26}+1$$

$$\underline{x^{29}+x^{27}+x^{24}}$$

$$x^{27}+x^{26}+x^{24}+1$$

$$\underline{x^{27}+x^{25}+x^{22}}$$

$$x^{26}+x^{25}+x^{24}+x^{22}+1$$

$$\underline{x^{26}+x^{24}+x^{21}}$$

$$x^{25}+x^{22}+x^{21}+1$$

$$\underline{x^{25}+x^{23}+x^{20}}$$

$$\cancel{x^{23}}+x^{22}+\cancel{x^{21}}+x^{20}+1$$

$$\underline{\cancel{x^{23}}+\cancel{x^{21}}+x^{18}}$$

$$x^{22}+x^{20}+x^{18}+1$$

$$\underline{x^{22}+x^{20}+x^{17}}$$

$$x^{18}+x^{17}+1$$

$$\underline{x^{18}+x^{16}+x^{13}}$$

$$x^{17}+x^{16}+x^{13}+1$$

$$\underline{x^{17}+x^{15}+x^{12}}$$

$$x^{16}+x^{15}+x^{13}+x^{12}+1$$

$$\underline{x^{16}+x^{14}+x^{11}}$$

$$x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+1$$

$$x^{10}+x^{9}+x^{6}+x^{5}+x^{3}+1$$

$$x^5+x^3+1 \;\overline{)\; x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+1}$$

$$\underline{x^{15}+x^{13}+x^{10}}$$

$$x^{14}+x^{12}+x^{11}+x^{10}+1$$

$$\underline{x^{14}+x^{12}+x^{9}}$$

$$x^{11}+x^{10}+x^{9}+1$$

$$\underline{x^{11}+x^{9}+x^{6}}$$

$$x^{10}+x^{6}+1$$

$$\underline{x^{10}+x^{8}+x^{5}}$$

$$x^{8}+x^{6}+x^{5}+1$$

$$\underline{x^{8}+x^{6}+x^{3}}$$

$$x^{5}+x^{3}+1$$

$$\underline{x^{5}+x^{3}+1}$$

$$0 \quad \checkmark$$

#12.

$1+x^2+x^5$

$1+x+x^2+x^3+x^5$

$1+x^3+x^5$

$1+x+x^2+x^4+x^5$

$1+x^2+x^3+x^4+x^5$

$1+x^3+\cancel{x^2}+x^4+x^5$

$P(\alpha)=0$

$1+\alpha+x^3=0$

#13

$P(X) = 1+X+X^3$

Power Rep.	Polynomial Rep.	3-tuple Rep.
0	0	$(0,0,0)$
1	1	$(1,0,0)$
α	α	$(0,1,0)$
α^2	α^2	$(0,0,1)$
α^3	$1+\alpha$	$(1,1,0)$
α^4	$\alpha+\alpha^2$	$(0,1,1)$
α^5	$1+\alpha+\alpha^2$	$(1,1,1)$
α^6	$1 \quad +\alpha^2$	$(1,0,1)$

Sketch:

$$\begin{aligned}\alpha^6 &= \alpha^3\alpha^3\\ &= (1+\alpha)(1+\alpha)\\ &= \alpha^2+1\end{aligned}$$

#14. $P(X) = 1+X^2+X^5 \rightarrow$ $P(\alpha)=0$

$1+\alpha^2+\alpha^5=0$

Power Rep.

0

1

α

α^2

α^3

α

Going to need more space...

#14. $P(X) = 1+X^2+X^5$ $\qquad P(\alpha)=0$

$\alpha^5 = 1+\alpha^2$

Power Rep.	Polynomial Rep.	5-tuple form
0	0	$(0,0,0,0,0)$
1	1	$(1,0,0,0,0)$
α	α	$(0,1,0,0,0)$
α^2	α^2	$(0,0,1,0,0)$
α^3	α^3	$(0,0,0,1,0)$
α^4	α^4	$(0,0,0,0,1)$
α^5	$1+\alpha^2$	$(1,0,1,0,0)$
α^6	$\alpha+\alpha^3$	$(0,1,0,1,0)$
α^7	$\alpha^2+\alpha^4$	$(0,0,1,0,1)$
α^8	$1+\alpha^2+\alpha^3$	$(1,0,1,1,0)$
α^9	$\alpha+\alpha^3+\alpha^4$	$(0,1,0,1,1)$
α^{10}	$1+\alpha^4$	$(1,0,0,0,1)$
α^{11}	$1+\alpha+\alpha^2$	$(1,1,1,0,0)$
α^{12}	$\alpha+\alpha^2+\alpha^3$	$(0,1,1,1,0)$
α^{13}	$\alpha^2+\alpha^3+\alpha^4$	$(0,0,1,1,1)$
α^{14}	$1+\alpha^2+\alpha^3+\alpha^4$	$(1,0,1,1,1)$
α^{15}	$1+\alpha+\alpha^2+\alpha^3+\alpha^4$	$(1,1,1,1,1)$
α^{16}	$1+\alpha+\alpha^3+\alpha^4$	$(1,1,0,1,1)$
α^{17}	$1+\alpha+\alpha^4$	$(1,1,0,0,1)$
α^{18}	$1+\alpha$	$(1,1,0,0,0)$
α^{19}	$\alpha+\alpha^2$	$(0,1,1,0,0)$
α^{20}	$\alpha^2+\alpha^3$	$(0,0,1,1,0)$
α^{21}	$\alpha^3+\alpha^4$	$(0,0,0,1,1)$
α^{22}	$1+\alpha^2+\alpha^4$	$(1,0,1,0,1)$
α^{23}	$1+\alpha+\alpha^2+\alpha^3$	$(1,1,1,1,0)$
α^{24}	$\alpha+\alpha^2+\alpha^3+\alpha^4$	$(0,1,1,1,1)$
α^{25}	$1+\alpha^3+\alpha^4$	$(1,0,0,1,1)$
α^{26}	$1+\alpha+\alpha^2+\alpha^4$	$(1,1,1,0,1)$
α^{27}	$1+\alpha+\alpha^3$	$(1,1,0,1,0)$
α^{28}	$\alpha+\alpha^2+\alpha^4$	$(0,1,1,0,1)$
α^{29}	$1+\alpha^3$	$(1,0,0,1,0)$
α^{30}	$\alpha+\alpha^4$	$(0,1,0,0,1)$

#14 (continued)

Minimum polynomial $\phi(X)$ of $\beta = \alpha^3$ $\quad (GF(2^5))$

$$\cancel{\beta^2 = \alpha^6 = (\alpha+\alpha^3), \quad \beta^3 = \alpha^9 = (\alpha+\alpha^3+\alpha^4), \quad \beta^4 = \alpha^{12} = (\alpha+\alpha^2+\alpha^3)}$$

$$\beta^2 = \alpha^6, \quad \beta^{2^2} = \alpha^{12}, \quad \beta^{2^3} = \alpha^{24}, \quad \beta^{2^4} = \alpha^{48} = \alpha^{11}$$

$$\phi(X) = a_0 + a_1 X + a_2 X^2 + a_3 X^3 + a_4 X^4 + X^5$$

$$\phi(\beta) = 0$$
$$= a_0 + a_1(\alpha^3) + a_2 \alpha^6 + a_3(\alpha^{12}) + a_4(\alpha^{24}) + \alpha^{11}$$

substituting in from the table...

$$0 = a_0 + a_1(\alpha^3) + a_2(\alpha+\alpha^3) + a_3(\alpha+\alpha^2+\alpha^3) + \ldots$$
$$a_4(\alpha+\alpha^2+\alpha^3+\alpha^4) + (1+\alpha+\alpha^2)$$

$$0 = a_0 + 1 + \alpha(a_2+a_3+a_4+1) + \alpha^2(a_3+a_4+1) + \alpha^3(a_1+a_2+a_3+a_4+1) + \ldots$$
$$\alpha^4(a_4)$$

$$\Rightarrow \left[\begin{array}{r} a_0+1=0 \\ a_2+a_3+a_4+1=0 \\ a_3+a_4+1=0 \\ a_1+a_2+a_3+a_4+1=0 \\ a_4=0 \end{array}\right] \rightarrow \left[\begin{array}{r} a_0=1 \\ a_2+a_3+1=0 \\ a_3+1=0 \\ a_1+a_2+a_3+1=0 \\ a_4=0 \end{array}\right] \rightarrow \left[\begin{array}{r} a_0=1 \\ a_2=0 \\ a_3=1 \\ a_1=0 \\ a_4=0 \end{array}\right]$$

$$\Rightarrow \boxed{\phi(x) = 1 + x^3 + x^5}$$

#8. $\left[\begin{array}{l} x + \alpha^5 y + z = \alpha^7 \\ x + \alpha y + \alpha^7 z = \alpha^9 \\ \alpha^2 x + y + \alpha^6 z = \alpha \end{array}\right.$ $\rightarrow$ $1+\alpha^7 = \alpha + \alpha^3$

$\Downarrow$

$$\left(\begin{array}{ccc|c} 1 & \alpha^5 & 1 & \alpha^7 \\ 1 & \alpha & \alpha^7 & \alpha^9 \\ \alpha^2 & 1 & \alpha^6 & \alpha \end{array}\right) \rightarrow \left(\begin{array}{ccc|c} 1 & \alpha^5 & 1 & \alpha^7 \\ 0 & \alpha^2 & 1+\alpha^7 & 1 \\ 0 & 1+\alpha^7 & \alpha^3 & \alpha^3 \end{array}\right)$$

$$\rightarrow \left(\begin{array}{ccc|c} 1 & \alpha^5 & 1 & \alpha^7 \\ 0 & 1 & \alpha^{14}+\alpha^{16} & \alpha^{13} \\ 0 & \alpha+\alpha^3 & \alpha^3 & \alpha^3 \end{array}\right) \rightarrow \left(\begin{array}{ccc|c} 1 & \alpha^5 & 1 & \alpha^7 \\ 0 & 1 & \alpha^7 & \alpha^{13} \\ 0 & \alpha+\alpha^3 & \alpha^3 & \alpha^3 \end{array}\right)$$

$$\rightarrow \left(\begin{array}{ccc|c} 1 & \alpha^5 & 1 & \alpha^7 \\ 0 & 1 & \alpha^7 & \alpha^{13} \\ 0 & 0 & \alpha^8+\alpha^{10}+\alpha^3 & \alpha^3+\alpha^{14}+\alpha^{16} \end{array}\right) \rightarrow \left(\begin{array}{ccc|c} 1 & \alpha^5 & 1 & \alpha^7 \\ 0 & 1 & \alpha^7 & \alpha^{13} \\ 0 & 0 & \alpha^{14} & 0 \end{array}\right)$$

$$\rightarrow \left(\begin{array}{ccc|c} 1 & \alpha^5 & 0 & \alpha^7 \\ 0 & 1 & 0 & \alpha^{13} \\ 0 & 0 & 1 & 0 \end{array}\right) \rightarrow \left(\begin{array}{ccc|c} 1 & 0 & 0 & \alpha^7+\alpha^{18} \\ 0 & 1 & 0 & 1+\alpha^2+\alpha^3 \\ 0 & 0 & 1 & 0 \end{array}\right)$$

$$\rightarrow \left(\begin{array}{ccc|c} 1 & 0 & 0 & 1+\alpha \\ 0 & 1 & 0 & 1+\alpha^2+\alpha^3 \\ 0 & 0 & 1 & 0 \end{array}\right) \Rightarrow \left[\begin{array}{l} x = 1+\alpha \\ y = 1+\alpha^2+\alpha^3 \\ z = 0 \end{array}\right]$$