HW 2 (Due date 24 April 2020)

1. (20 pts) Prove $[f(X)]^{2\wedge l} = f(X^{2\wedge l})$ over **GF(2)**.

   l = 1

   $$f(X)=\sum_{n=0}^{k} b_n X^n, b_n \in \{0,1\}$$

   $$[f(X)]^2=\sum_{t=0}^{k} b_t X^t (\sum_{n=0}^{k} b_n X^n)$$

   $$[f(X)]^2=\sum_{t=0}^{k} X^t (\sum_{n=0}^{k} b_n X^n), b_t=1$$

   $$[f(X)]^2=\sum_{t=0}^{k} X^{2t}+\sum_{t=0}^{k} (\sum_{n=0}^{k} b_n X^{n+t}), b_t=1, n\neq t$$

   $$[f(X)]^2=\sum_{t=0}^{k} X^{2t}+2\sum_{t=0}^{k} (\sum_{n=0}^{m} b_n X^{n+t}), b_t=1, m<t$$

   $$[f(X)]^2=\sum_{t=0}^{k} X^{2t}, b_t=1$$

   $$[f(X)]^2=\sum_{t=0}^{k} b_t X^{2t}, b_n \in \{0,1\}=f(X^2)$$

   if l = p

   $[f(X)]^{2^p}=f(X^{2^p})$ is ture

   then l = p + 1

   $$[f(X)]^{2^{p+1}}=([f(X)]^{2^p})^2=[f(X^{2^p})]^2=\sum_{t=0}^{k} b_t X^{2^p*2}, b_n \in \{0,1\}=f(X^{2^{p+1}})$$ is ture

2. (20 pts) Construct the Galois filed GF(32) constructed with primitive polynomial $X^5 + X^2 + 1$.

0	0	(0,0,0,0,0)
a^0	1	(0,0,0,0,1)
a^1	a^1	(0,0,0,1,0)
a^2	a^2	(0,0,1,0,0)
a^3	a^3	(0,1,0,0,0)
a^4	a^4	(1,0,0,0,0)
a^5	a^2+1	(0,0,1,0,1)
a^6	a^3+a	(0,1,0,1,0)

a^{7}	$a^{4}+a^{2}$	(1,0,1,0,0)
a^{8}	$a^{3}+a^{2}+1$	(0,1,1,0,1)
a^{9}	$a^{4}+a^{3}+a$	(1,1,0,1,0)
a^{10}	$a^{4}+1$	(1,0,0,0,1)
a^{11}	$a^{2}+a+1$	(0,0,1,1,1)
a^{12}	$a^{3}+a^{2}+a$	(0,1,1,1,0)
a^{13}	$a^{4}+a^{3}+a^{2}$	(1,1,1,0,0)
a^{14}	$a^{4}+a^{3}+a^{2}+1$	(1,1,1,0,1)
a^{15}	$a^{4}+a^{3}+a^{2}+a+1$	(1,1,1,1,1)
a^{16}	$a^{4}+a^{3}+a+1$	(1,1,0,1,1)
a^{17}	$a^{4}+a+1$	(1,0,0,1,1)
a^{18}	$a+1$	(0,0,0,1,1)
a^{19}	$a^{2}+a$	(0,0,1,1,0)
a^{20}	$a^{3}+a^{2}$	(0,1,1,0,0)
a^{21}	$a^{4}+a^{3}$	(1,1,0,0,0)
a^{22}	$a^{4}+a^{2}+1$	(1,0,1,0,1)
a^{23}	$a^{3}+a^{2}+a+1$	(0,1,1,1,1)
a^{24}	$a^{4}+a^{3}+a^{2}+a$	(1,1,1,1,0)
a^{25}	$a^{4}+a^{3}+1$	(1,1,0,0,1)
a^{26}	$a^{4}+a^{2}+a+1$	(1,0,1,1,1)
a^{27}	$a^{3}+a+1$	(0,1,0,1,1)
a^{28}	$a^{4}+a^{2}+a$	(1,0,1,1,0)
a^{29}	$a^{3}+1$	(0,1,0,0,1)
a^{30}	$a^{4}+a$	(1,0,0,1,0)

3. Using the Galois filed GF(32) constructed with primitive polynomial $X^5 + X^2 + 1$ to finish the calculation below.

   a. (20 pts) Find the root of $f(X) = X^4 + \alpha^{27}X^3 + \alpha^{6}X$.

$$X^4+(0,1,0,1,1)X^3+(0,1,0,1,0)X=(0,0,0,0,0)$$

(0,0,0,0,0) is one of the root

b. (20 pts) Solve the system

$$\alpha^{21}\boldsymbol{X}+\alpha\boldsymbol{Y}+\boldsymbol{Z}=1$$

$$\boldsymbol{X}+\alpha^{13}\boldsymbol{Y}+\alpha^{6}\boldsymbol{Z}=\alpha^{10}$$

$$\boldsymbol{X}+\boldsymbol{Y}+\alpha^{16}\boldsymbol{Z}=\alpha^{20}$$

$$\begin{bmatrix} a^{21} & a & 1 & a^{0} \\ 1 & a^{13} & a^{6} & a^{10} \\ 1 & 1 & a^{16} & a^{20} \end{bmatrix}=\begin{bmatrix} 0 & a+a^{21} & 1+a^{37} & 1+a^{41} \\ 0 & a^{13}+a^{0} & a^{6}+a^{16} & a^{10}+a^{20} \\ 1 & 1 & a^{16} & a^{20} \end{bmatrix}$$

$$\begin{bmatrix} 0 & a^{9} & a^{27} & a^{4} \\ 0 & a^{14} & a^{10} & a^{14} \\ 1 & 1 & a^{16} & a^{20} \end{bmatrix}$$

$$\begin{bmatrix} 0 & a^{9} & a^{27} & a^{4} \\ 0 & a^{14}+a^{14} & a^{10}+a^{32} & a^{14}+a^{9} \\ 1 & 1 & a^{16} & a^{20} \end{bmatrix}=\begin{bmatrix} 0 & a^{9} & a^{27} & a^{4} \\ 0 & 0 & a^{17} & a^{11} \\ 1 & 1 & a^{16} & a^{20} \end{bmatrix}$$

$$a^{17}Z=a^{11}$$

$$Z=a^{25}$$

$$a^{9}Y+a^{52}=a^{4}$$

$$a^{9}Y=a^{3}$$

$$Y=a^{25}$$

$$X+a^{25}+a^{41}=a^{20}$$

$$X=a^{2}$$

4. (20 pts) Find the number of possible generator matrices with orthogonal rows for the codebook and explain the details for your answer.

Messages	Codewords
(m_0, m_1, m_2)	(c_0, c_1,…, c_5)

(0 0 0)	(0 0 0 0 0 0)
(0 0 1)	(1 1 0 0 0 1)
(0 1 0)	(1 0 1 0 1 0)
(0 1 1)	(0 1 1 0 1 1)
(1 0 0)	(0 1 1 1 0 0)
(1 0 1)	(1 0 1 1 0 1)
(1 1 0)	(1 1 0 1 1 0)
(1 1 1)	(0 0 0 1 1 1)

$C=(c_0,c_1,\ldots,c_5)$

$G: generator$

$M*G=C$

Choose message vectors (1 0 0), (0 1 0) and (0 0 1) to combine the three-dimension identity matrix.

So the generator matrices is the combination of row vectors which pick up from code words.

But there are not two vectors in the codeword set which dot product equal to zero. So there is not a generator matrices with orthogonal rows.