ECE454/544: Fault-Tolerant Computing & Reliability Engineering
(Fall 2022)

Homework #3 Solution
(50 points)

1. **(30 points)** ***Non-separable*** **Cyclic Code:**
   1) Design a combinatorial circuit that is capable of encoding four-bit information words into *non-separable* cyclic code words using the generator polynomial $G(X)=1+X+X^2+X^5$. **(20 points)**
   2) Show the resulting code word for the data word (d3 d2 d1 d0) = (1011). **(10 points)**

Solution:

Information words : 4 bits $\Rightarrow k=4$
$G(x) = 1+x+x^2+x^5 \Rightarrow n-k=5$
$\Rightarrow n=9$

Data polynomial: $D(x) = d_0 + d_1 x + d_2 x^2 + d_3 x^3$

Generator polynomial: $G(x) = 1 + x + x^2 + x^5$

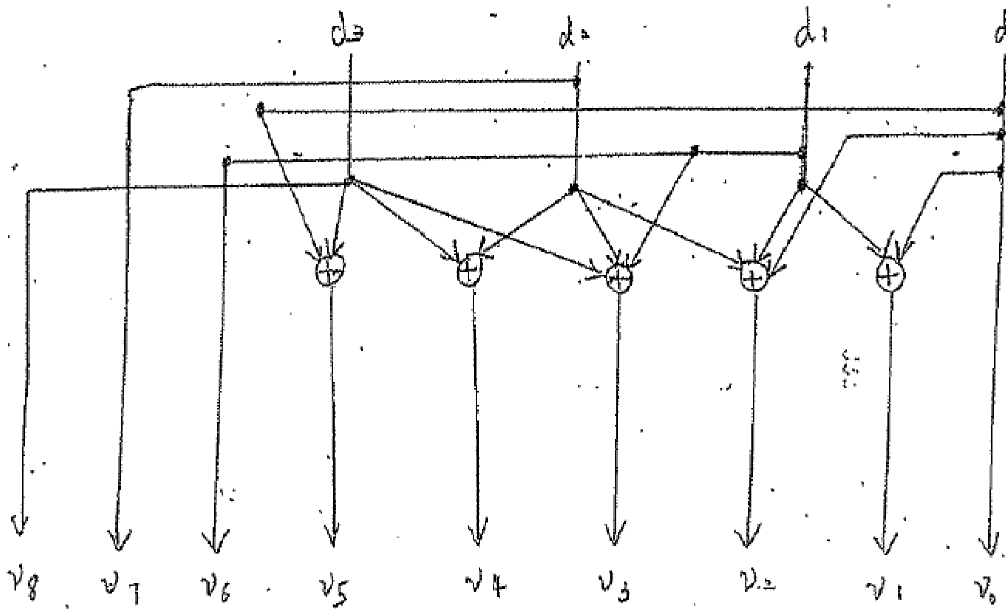
Code polynomial: $V(x) = D(x)\cdot G(x) = V_0 + V_1 x + V_2 x^2 + \cdots + V_8 x^8$

$$V(x) = D(x)\cdot G(x) = (d_0 + d_1 x + d_2 x^2 + d_3 x^3)(1 + x + x^2 + x^5)$$
$$= d_0 + d_0 x + \underline{d_0 x^2} + d_0 x^5 + d_1 x + \underline{d_1 x^2} + \underline{d_1 x^3} + d_1 x^6 + \underline{d_2 x^2} + d_2 x^3 + d_2 x^4 + d_2 x^7 + d_3 x^3 + d_3 x^4 + d_3 x^5 + d_3 x^8$$
$$= d_0 + (d_0 + d_1)x + (d_0 + d_1 + d_2)x^2 + (d_1 + d_2 + d_3)x^3 + (d_2 + d_3)x^4 + (d_0 + d_3)x^5 + d_1 x^6 + d_2 x^7 + d_3 x^8$$

So, the code word is given by:

$v = (v_0, v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8)$
$= (d_0, (d_0+d_1), (d_0+d_1+d_2), (d_1+d_2+d_3), (d_2+d_3), (d_0+d_3), d_1, d_2, d_3)$

Thus, this non-separable cyclic code can be implemented using the following combinatorial circuit composed of EXCLUSIVE-OR gates only:



$\oplus$: EXCLUSIVE-OR gate implementing modulo-2 addition

For data word 1011, we have

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

$$V(x) = D(x) \cdot G(x) = (1 + x + x^3)(1 + x + x^2 + x^5)$$

$$= 1 + x^4 + x^6 + x^8$$

So, the code word for 1011 is

$$v = (v_8, v_7, \ldots, v_1, v_0)$$

$$= (101010001)$$

2. **(20 points)** ***Separable*** **Cyclic Code:**
Show the *separable* cyclic code word for the data word (d3 d2 d1 d0) = (1011) using the generator polynomial $G(X)=1+X+X^2+X^5$.

Solution:

For data word 1011, we have

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

To construct separable cyclic code, we compute:

① $x^{n-k} \cdot D(x) = x^5(1+x+x^3) = x^5+x^6+x^8$

② Find the remainder $R(x)$ of the division $x^{n-k}D(x)/G(x)$

$$\begin{array}{r|l} & x^3+x \\ \hline x^5+x^2+x+1 & x^8+x^6+x^5 \\ & x^8+x^5+x^4+x^3 \\ \hline & x^6+x^4+x^3 \\ & x^6+x^3+x^2+x \\ \hline & x^4+x^2+x \rightarrow R(x) \end{array}$$

So, $R(x) = x^4+x^2+x$

③ $V(x) = x^{n-k}D(x) + R(x) = x^5+x^6+x^8+x^4+x^2+x$

$$= x^8+x^6+x^5+x^4+x^2+x$$

So, the separate cyclic code word for 1011 is:

$v = (v_8, v_7, \ldots v_1, v_0)$

$= (101110110)$