ELEC 6131 – Error Detecting and Correcting Codes

Final Exam

April 12, 2016

1) Consider the Galois field GF (2^4) generated by the polynomial $p(x) = x^4 + x + 1$.

   a) Find the generating polynomial of (15, 13) RS code over this field (5 Marks).

$$g(x) = (x + \alpha)(x + \alpha^2) = x^2 + (\alpha + \alpha^2)x + \alpha^3$$

   From:

Three representations for the elements of $GF(2^4)$ generated by $p(X) = 1 + X + X^4$.

Power representation	Polynomial representation	4-Tuple representation
0	0	(0 0 0 0)
1	1	(1 0 0 0)
α	α	(0 1 0 0)
α^2	α^2	(0 0 1 0)
α^3	α^3	(0 0 0 1)
α^4	$1 + \alpha$	(1 1 0 0)
α^5	$\alpha + \alpha^2$	(0 1 1 0)
α^6	$\alpha^2 + \alpha^3$	(0 0 1 1)
α^7	$1 + \alpha + \alpha^3$	(1 1 0 1)
α^8	$1 + \alpha^2$	(1 0 1 0)
α^9	$\alpha + \alpha^3$	(0 1 0 1)
α^{10}	$1 + \alpha + \alpha^2$	(1 1 1 0)
α^{11}	$\alpha + \alpha^2 + \alpha^3$	(0 1 1 1)
α^{12}	$1 + \alpha + \alpha^2 + \alpha^3$	(1 1 1 1)
α^{13}	$1 + \alpha^2 + \alpha^3$	(1 0 1 1)
α^{14}	$1 + \alpha^3$	(1 0 0 1)

   we get: $\alpha + \alpha^2 = \alpha^5$.

   So,

$$g(x) = x^2 + \alpha^5 x + \alpha^3$$

   b) What is the error correcting capability of this code? Erasure correcting capability? (1 Mark)

   $n - k = 15 - 13 = 2 = 2t$. So, the code can correct one error. It can correct two erasures.

   c) Encode the sequence $u(x) = x^3$ in a systematic form. (3 Marks)

$$x^{n-k}u(x) = x^{15-13}x^3 = x^5$$

   Dividing x^5 by $g(x) = x^2 + \alpha^5 x + \alpha^3$, we get:

$$x^5 = (x^3 + \alpha^5 x^2 + \alpha^{12} x + 1)(x^2 + \alpha^5 x + \alpha^3) + \alpha^{10} x + \alpha^3$$

   So parity is $p(x) = \alpha^{10} x + \alpha^3$ and the codeword is:

$$v(x) = x^5 + \alpha^{10} x + \alpha^3.$$

   d) Decode the received sequence $r(x) = e_1 x + e_2 x^3$ where e_1 and e_2 are erased symbols (3 Marks).

   Compute the syndromes:

$$S_1 = r(\alpha) = e_1\alpha + e_2\alpha^3 = 0$$

and

$$S_2 = r(\alpha^2) = e_1\alpha^2 + e_2\alpha^6 = 0$$

It is easy to see that $e_1 = e_2 = 0$ soles the above system of equations.

2) Consider the Galois field GF (2^4) generated by the polynomial $p(x) = x^4 + x + 1$. Find the generator polynomial of a primitive binary BCH code with n = 15 and t = 3 (7 Marks). What is the minimum distance and the rate of the resulting code (3 Marks)?

$$g(x) = \phi_1(x)\phi_3(x)\phi_5(x)$$

Using the table:

Conjugate Roots	$\emptyset(X)$
0	X
1	$X + 1$
$\alpha, \alpha^2, \alpha^4, \alpha^8$	$X^4 + X + 1$
$\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$	$X^4 + X^3 + X^2 + X + 1$
α^5, α^{10}	$X^2 + X + 1$
$\alpha^7, \alpha^{11}, \alpha^{13}, \alpha^{14}$	$X^4 + X^3 + 1$

we get:

$$\phi_1(x) = X^4 + X + 1$$

$$\phi_3(x) = X^4 + X^3 + X^2 + X + 1$$

$$\phi_5(x) = X^2 + X + 1$$

So,

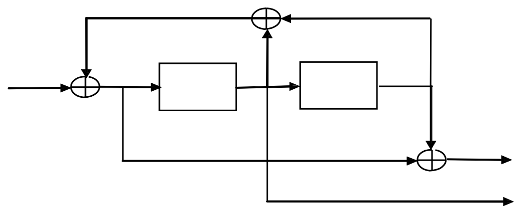
$$g(x) = X^{10} + X^8 + X^5 + X^4 + X^2 + X + 1$$

The distance of the code is 7.

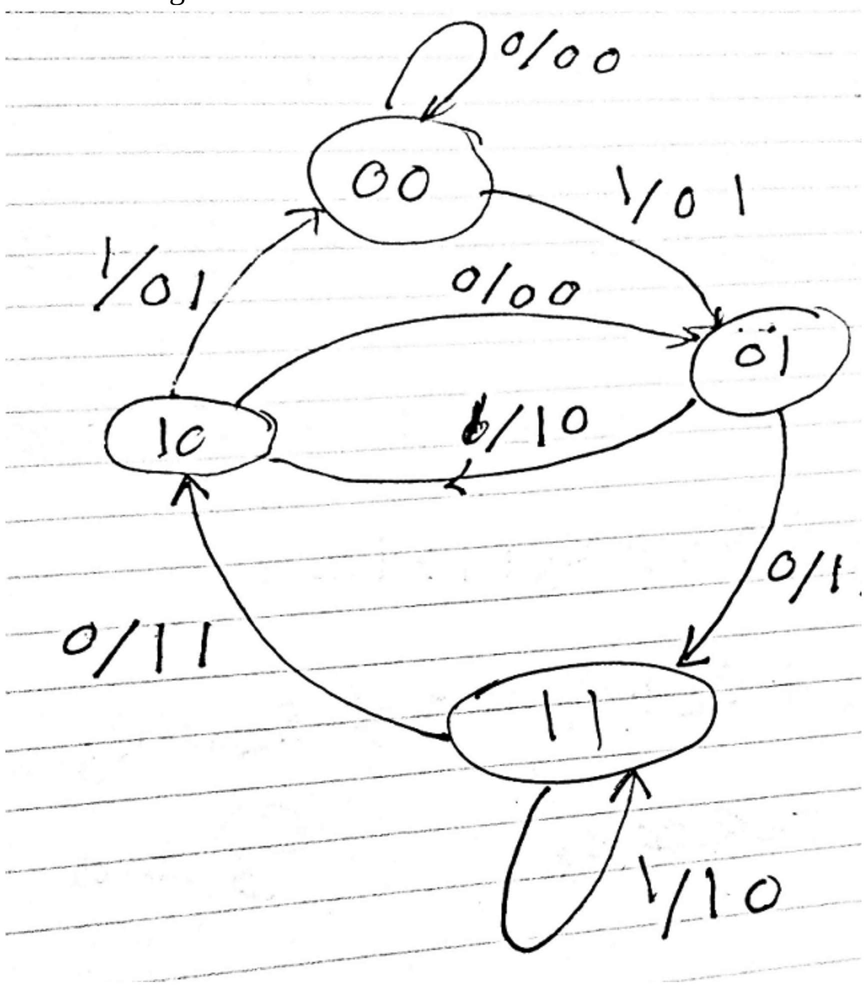
$$n - k = 10.$$

So $k = 15 - 10$=5. The code is $(15, 5)$ with rate 1/3.

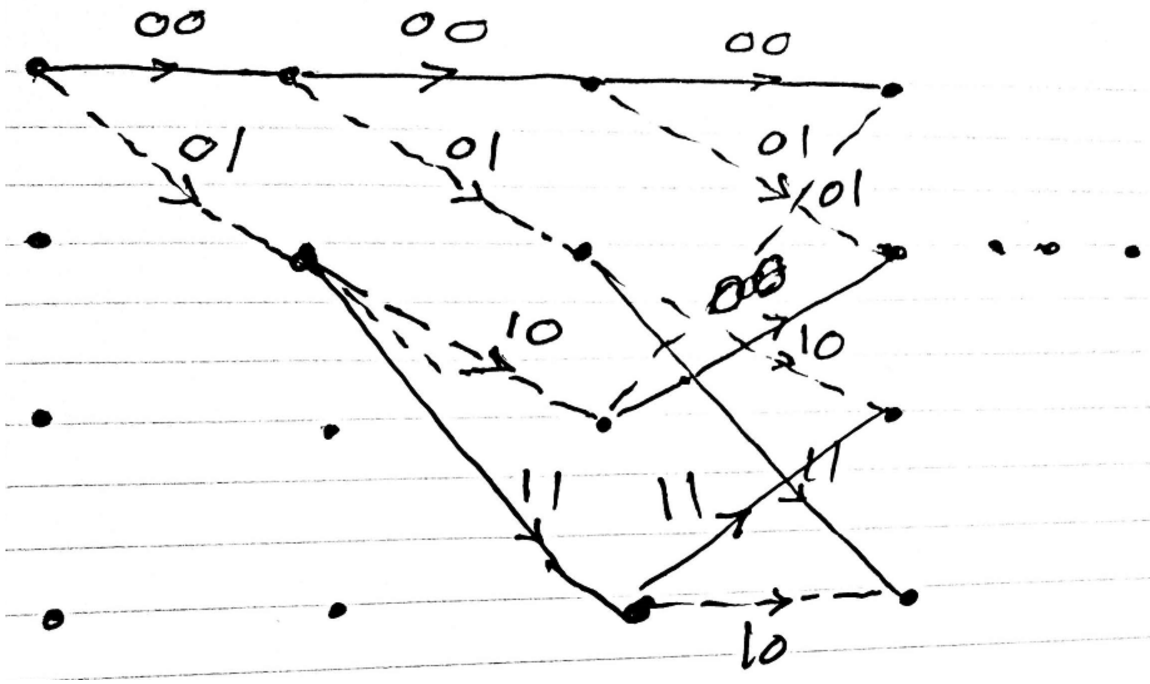
3) Consider the following convolutional encoder with generating function $G(D) = \left[\frac{1+D^2}{1+D+D^2}, \frac{D}{1+D+D^2} \right]$



a) Draw the trellis diagram for the code (2 Marks).
The state diagram is:



The trellis diagram is:

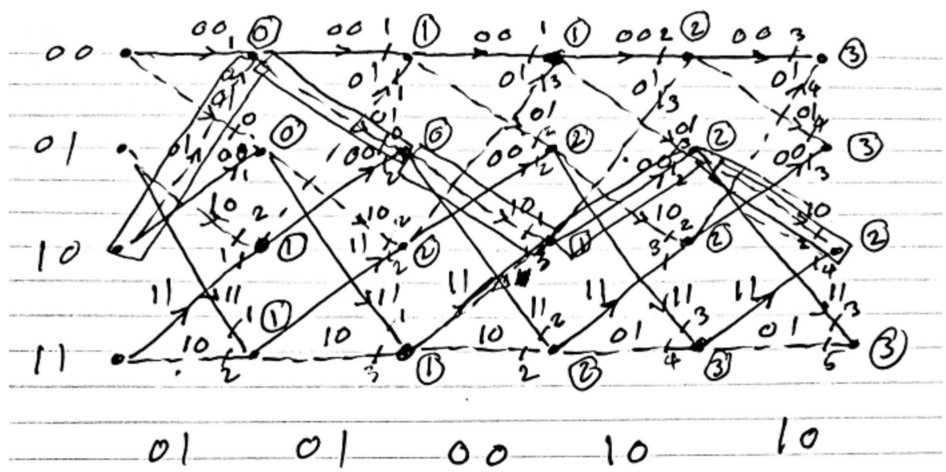


b) What is the minimum free distance of the code (2 Marks).

$$d_{free} = 3$$

c) Encode 1101011 staring from state zero (2 Marks).
01,10,00,10,00,10,01

d) Using the Viterbi Algorithm decode 0101001010 (4 Marks).
Note: The encoding has started from an unknown state.



The answer is 11101.

4) What is a catastrophic encoder? What is the condition for a convolutional encoder not to be catastrophic? (3 Marks).
A catastrophic encoder is one that generates outputs with finite distance for inputs with infinite distance.
In order for a code to be non-catastrophic, the greatest common divisor of its generating polynomials should be either one or a one shifted by i, i.e., D^i.

5) Let x and y be independent binary random variables.

a) Find the LLR of x if $P(x=0)=0.5$ (1 Mark).

$$LLR(x) = log\frac{0.5}{0.5} = 0$$

b) Find the LLR of x if $x=1$, i.e., $P(x=0)=0$ (1 Mark).

$$LLR(x) = log\frac{0}{1} = -\infty$$

c) Find the LLR of x if $x=0$ (1 Mark).

$$LLR(x) = log\frac{1}{0} = \infty$$

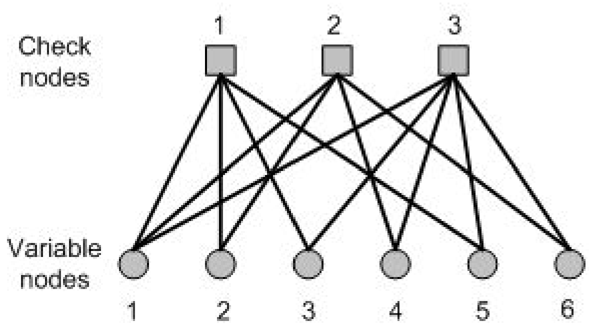
d) Find the LLR of $z = x \oplus y$ if $P(x=0)=P(y=1)=0.25$ (3 Marks).

$$P(x=0)=0.25, P(x=1)=0.75$$
$$P(y=0)=0.75, P(y=1)=0.25$$
$$P(z=0)=P(x=0,y=0)+P(x=1,y=1)$$
$$=0.25\times 0.75+0.75\times 0.25=0.375$$

So,

$$LLR(z) = log\frac{0.375}{0.625} \approx -0.51$$

6) Consider a code with the following Tanner graph:



a) Write the parity check matrix of the code (2 Marks).

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

b) What are the row and column degree distribution functions (2 Marks)?

c) Find the rate of the code using the result of part b (2 Marks) and compare with the design rate.

$\lambda_2 = \frac{10}{13}, \lambda_3 = \frac{3}{13}$, and $\lambda_i = 0, i \neq 2 \ or \ i \neq 3$. So,

$$\lambda(x) = \frac{10}{13}x + \frac{3}{13}x^2$$

Therefore, $\int_0^1 \lambda(x)dx = \frac{10}{13\times 2}x^2 + \frac{3}{13\times 3}x^3 \ (at\, x=1) = \frac{6}{13}$

$\rho_4 = \frac{8}{13}, \rho_5 = \frac{5}{13}$ and $\rho_i = 0, i \neq 4 \ or \ i \neq 5$. So,

$$\rho(x) = \frac{8}{13}x^3 + \frac{5}{13}x^4$$

Therefore, $\int_0^1 \rho(x)dx = \frac{8}{13\times4}x^4 + \frac{5}{13\times5}x^5$ (at $x = 1$)$= \frac{3}{13}$

So, the rate is:

$$R = 1 - \frac{\frac{3}{13}}{\frac{6}{13}} = \frac{1}{2}$$

that is the same as the design rate.

d) Is 010111 a codeword? (1 Mark).

$c_1 = 0$, $c_2 = 1$, $c_3 = 1$. So, it is not a codeword.

e) Decode e1ee11 where e is an erasure (2 Marks).

$$e_1 + 1 + e_2 + 1 = 0 \Rightarrow e_1 + e_2 = 0$$

$$e_1 + 1 + e_3 + 1 = 0 \Rightarrow e_1 + e_3 = 0$$

$$e_1 + e_2 + e_3 + 1 + 1 = 0 \Rightarrow e_1 + e_2 + e_3 = 0$$

Substituting the first equation into third, we get $e_3 = 0$.

Substituting $e_3 = 0$ into the second equation, we get $e_1 = 0$.

Substituting $e_1 = 0$ into the first equation, we get $e_2 = 0$.

So, $e_1 = e_2 = e_3 = 0$ and the decoded codeword is 010011.