ELC 6131 – Error Detecting and Correcting Codes

Final Exam

April 28, 2015

1)

a) List all elements of GF(2^3) generated by $p(x) = x^3 + x + 1$ (1 Mark).

0	0	000
1	α^0	001
α	α^1	010
α^2	α^2	100
α^3	$\alpha + 1$	011
α^4	$\alpha^2 + \alpha$	110
α^5	$\alpha^2 + \alpha + 1$	111
α^6	$\alpha^2 + 1$	101

b) Find the generating polynomial of (7, 5) RS code over GF(2^3) (3 Marks).

$$g(x) = (x + \alpha)(x + \alpha^2) = x^2 + (\alpha^2 + \alpha)x + \alpha^3 = x^2 + \alpha^4 x + \alpha^3.$$

c) Encode the binary sequence 010101010101010 in systematic form using the above code (3 Marks).

$$u(x) = \alpha x^4 + \alpha^6 x^3 + \alpha x^2 + \alpha^6 x + \alpha$$

$$x^2 u(x) = \alpha x^6 + \alpha^6 x^5 + \alpha x^4 + \alpha^6 x^3 + \alpha x^2$$

Dividing $x^7 + 1$ by $\alpha x^6 + \alpha^6 x^5 + \alpha x^4 + \alpha^6 x^3 + \alpha x^2$, we get:

$$q(x) = \alpha x^5 + \alpha x^3 + \alpha^5 x^2 + 1$$

and remainder:

$$p(x) = \alpha^6 x + x^4$$

So, the codeword is:

$$v(x) = \alpha x^6 + \alpha^6 x^5 + \alpha x^4 + \alpha^6 x^3 + \alpha x^2 + \alpha^6 x + \alpha^4$$

Or,

$$v = (110,101,010,101,010,101,010).$$

d) Decode 000000000101000000000 (3 Marks)

$$r(x) = \alpha^6 x^3$$

Substituting α and α^2 in $r(x)$, we get:

$$S_1 = r(\alpha) = \alpha^9 = \alpha^2 \text{ and}$$

$$S_2 = r(\alpha^2) = \alpha^{12} = \alpha^5.$$

$$\sigma(x) = \sigma_0 + \sigma_1 x = 1 + \sigma_1 x.$$

The Newton Equation is:

$$S_2 + \sigma_1 S_1 = 0.$$

So,

$$\sigma_1 = \frac{S_2}{S_1} = \alpha^3.$$

Therefore,

$$\sigma(x) = 1 + \alpha^3 x$$

So the root of $\sigma(x)$ is α^4. Therefore, the error is at position X^3. It is not difficult to see that the error value is α^6 and the corrected information is all zero sequence.

2) Derive the generating polynomial of double-error correcting primitive BCH code of length 15 (7 Marks). Draw the systematic encoder for this code (2 Marks). What is the rate of the code (1 Mark)?

$$t = 2 \Rightarrow 2t = 4.$$

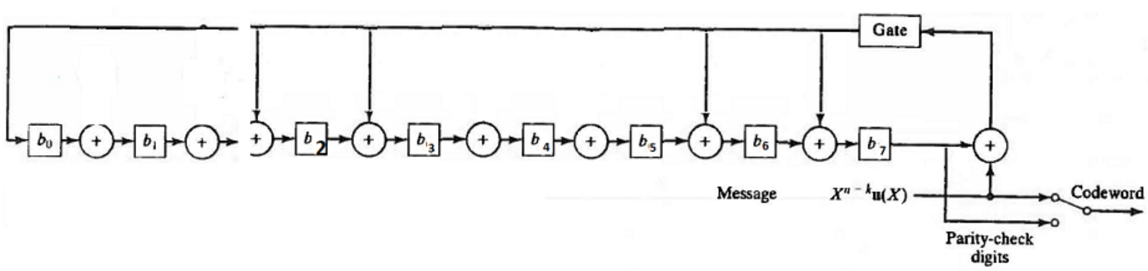
So,

$$g(x) = LCM[\phi_1(x), \phi_2(x), \phi_3(x), \phi_4(x)] = \phi_1(x)\phi_3(x).$$
$$g(x) = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1).$$
$$g(x) = x^8 + x^7 + x^6 + x^4 + 1.$$

TABLE 2.9: Minimal polynomials of the elements in $GF(2^4)$ generated by $p(X) = X^4 + X + 1$.

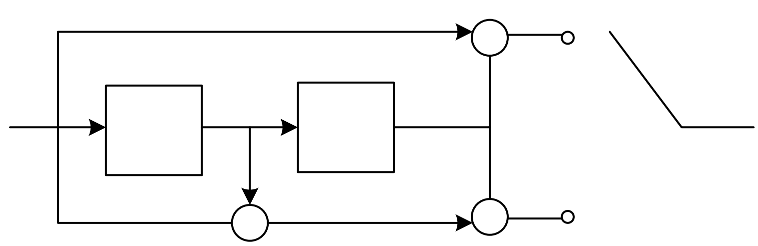
Conjugate roots	Minimal polynomials
0	X
1	$X+1$
$\alpha, \alpha^2, \alpha^4, \alpha^8$	X^4+X+1
$\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$	$X^4+X^3+X^2+X+1$
α^5, α^{10}	X^2+X+1
$\alpha^7, \alpha^{11}, \alpha^{13}, \alpha^{14}$	X^4+X^3+1

The encoder is:

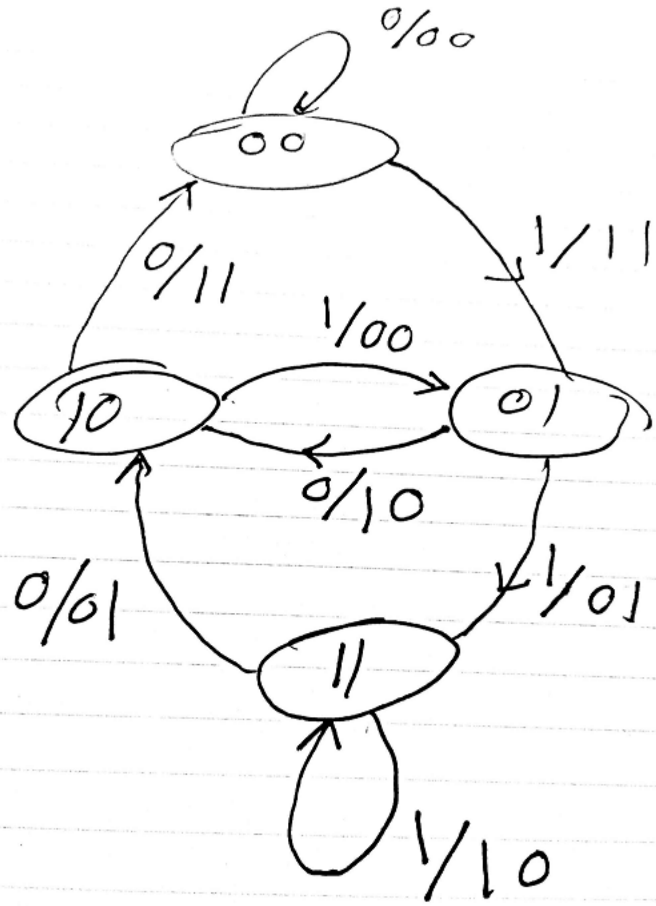


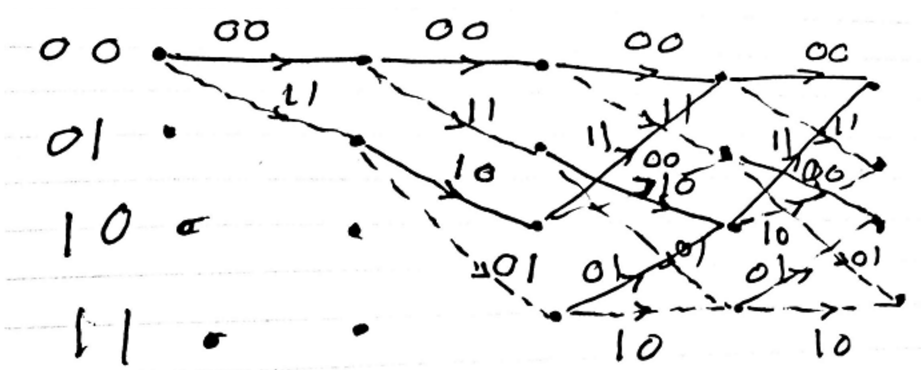
The rate is $r = \frac{7}{15}$.

3) Consider the following convolutional encoder:



a) Draw the trellis diagram for the code (2 Marks).



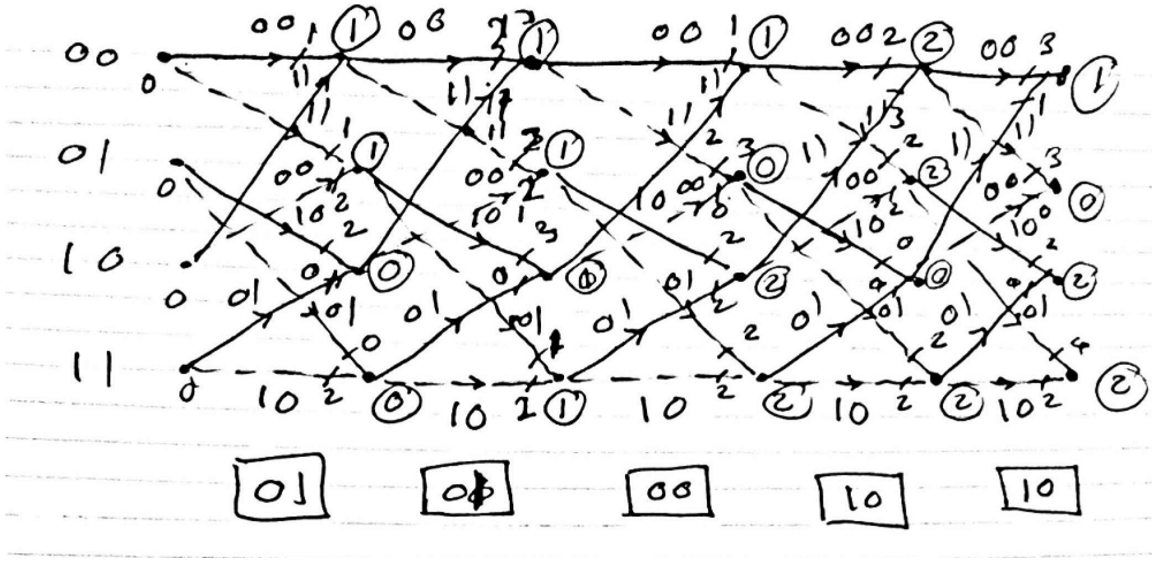


b) What is the minimum free distance of the code (2 Marks).

$$d_{free} = 5$$

c) Encode 1101011 staring from state zero (2 Marks).
11,01,01,00,10,00,01

d) Using the Viterbi Algorithm decode 0101001010 (4 Marks).
Note: The encoding has started from an unknown state.
Answer: 10101 starting from state 11.



4) Let x_1 and x_2 be two independent binary random variables and $y = x_1 \oplus x_2$. Let λ_1 and λ_2 be the *Log-Likelihood Ratio* (LLR) of x_1 and x_2, respectively.

a) Find the LLR of y (5 Marks).

Let $P(x_1 = 0) = p$ and $P(x_2 = 0) = q$ then:

$$\lambda_1 = log\frac{p}{1-p} \text{ and } \lambda_2 = log\frac{q}{1-q}$$

or,

$$p = \frac{e^{\lambda_1}}{1+e^{\lambda_1}} \text{ and } q = \frac{e^{\lambda_2}}{1+e^{\lambda_2}}$$

The LLR for y is:

$$\lambda = log\frac{P(y=0)}{P(y=1)}.$$

where,

$$P(y = 0) = pq + (1-p)(1-q) = 1 + 2pq - p - q$$

and

$$P(y = 1) = p + q - 2pq.$$

So,

$$\lambda = log\left[\frac{1 + 2pq - p - q}{-2pq + p + q}\right] = log\left[\frac{1}{p + q - 2pq} - 1\right]$$

or,

$$\lambda = log\left[\frac{1 + e^{\lambda_1+\lambda_2}}{e^{\lambda_1} + e^{\lambda_2}}\right]$$

b) Find the LLR of y for $\lambda_1 = 3$ and $\lambda_2 = -1$ (2 Marks). What is the probability that y is equal to zero? (1 Mark)

$$\lambda = log\left[\frac{1 + e^{3-1}}{e^3 + e^{-1}}\right] = -0.89$$

$$P(y=0) = \frac{e^{-0.89}}{1+e^{-0.89}} = 0.29$$

c) For a given λ_1, find λ_2 such that $P(y=0) = P(y=1) = 0.5$ (2 Mark)
We need to have $\lambda = 0$. Or, equivalently, we need:

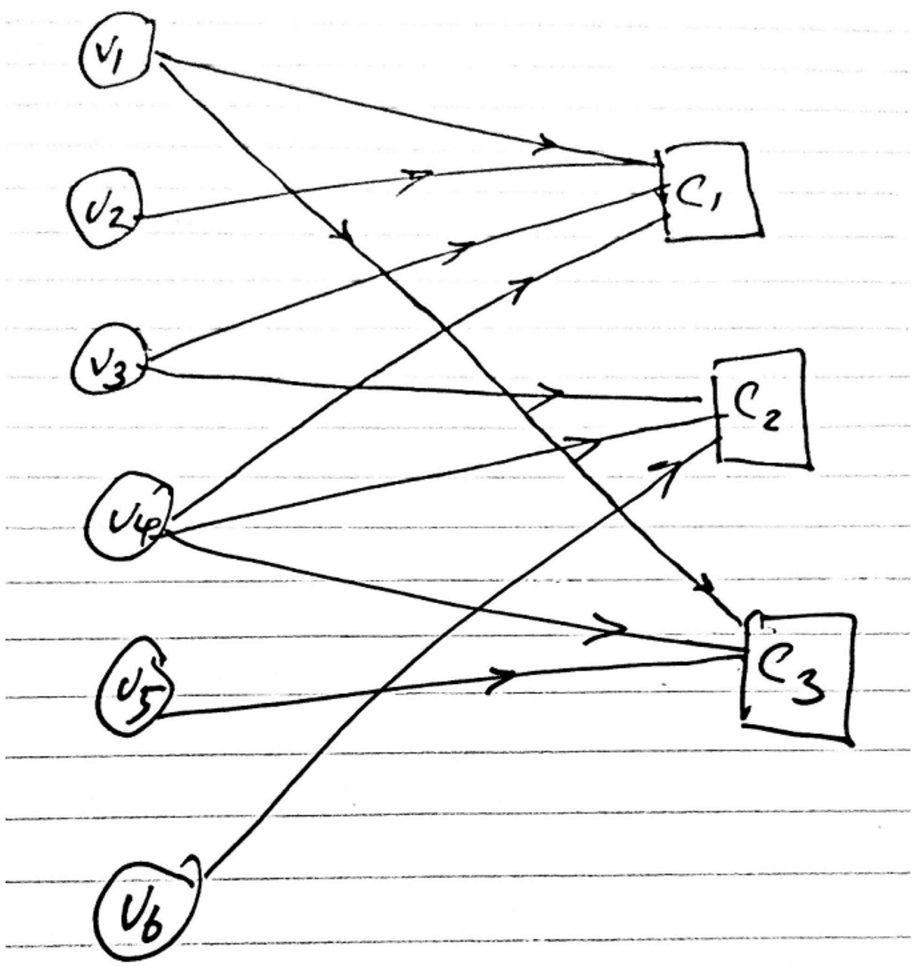
$$\frac{1+e^{\lambda_1}e^{\lambda_2}}{e^{\lambda_1}+e^{\lambda_2}} = 1.$$

If $\lambda_1 \neq 0$, we need to have $\lambda_2 = 0$. If $\lambda_1 = 0$, any value of λ_2 is acceptable.

5) Consider a code with the parity check matrix:

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}.$$

a) Draw the bi-partite (Tanner) graph for this code (2 Marks).



b) Find the rate of the code (3 Marks).
R=1/2

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

Yes.

d) Decode e1ee11 where e is an erasure (2 Marks).
Answer: 010111

e) Find a very **SIMPLE** encoding rule for this code (2 Marks). (by simple, I mean intuitive).
Answer: Use v_1, v_3, v_4 as systematic part and v_2, v_5, v_6 as parity. This means that first put the input bits at locations v_1, v_3, v_4 and zero in locations v_2, v_5, v_6 and compute check nodes c_1, c_2, c_3. If any of check nodes is one put a one on the single line connecting to it.