Ho Yau
6398723

University of Surrey
Department of Electrical and Electronic Engineering

EEE2040 Final Summative Assignment

1. **In a certain city, three car brands A, B, and C have 20%, 30% and 50% of the market share, respectively. The probabilities that a car will need a major repair during its first year of purchase are 0.05, 0.10 and 0.15, respectively.**

   a) **What is the probability that a car in this city will need a major repair during its first year of purchase?**

   Let:
   A be the event "Car is made by manufacturer A";
   B be the event "Car is made by manufacturer B";
   C be the event "Car is made by manufacturer C";
   D be the event "Car needs a major repair during its first year of purchase".

$$P(D) = 0.2\times0.05 + 0.3\times0.1 + 0.5\times0.15$$

$$= 0.115$$

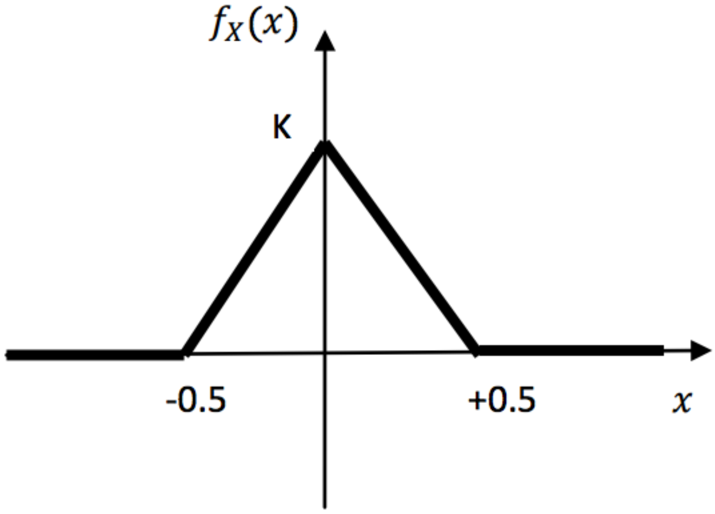
   b) **If a car in this city needs a major repair during its first year of purchase, what is the probability that it is made by manufacturer A?**

$$P(A|D) = \frac{P(D|A)P(A)}{P(D)}$$

$$= \frac{0.05 \times 0.2}{0.115}$$

$$= 0.0870$$

2. **A random variable X is defined by the following PDF:**



   a) **Find the value of K.**
   The total area of a PDF must be 1 since $0 \leq P(x) \leq 1$.
   Therefore,

$$\frac{K}{2} = 1$$

$$K = 2$$

b) Determine $P(X > 0.25)$.

The height of PDF at $X = 0.25$ is simply $\frac{K}{2} = 1$.

$$P(X > 0.25) = \frac{0.25\ \times 1}{2}$$

$$= 0.125$$

c) Determine $P(X > 0 \mid X < 0.25)$.

$$P(X > 0 \mid X < 0.25) = \frac{2 \times 0.5}{2} - 0.125$$

$$= 0.375$$

d) What is $f_x(x|X > 0)$**?**

$$\frac{f_x(x|X > 0)}{\mathrm{x} - 0.5} = \frac{2}{-0.5}$$

$$f_x(x|X > 0) = -4x + 2$$

e) Determine $E(X|X > 0)$.

$$E(X|X > 0) = \int_0^{0.5} x(-4x + 2)\ dx$$

$$= -\frac{4}{3}0.5^3 + 0.5^2$$

$$= 0.0833$$

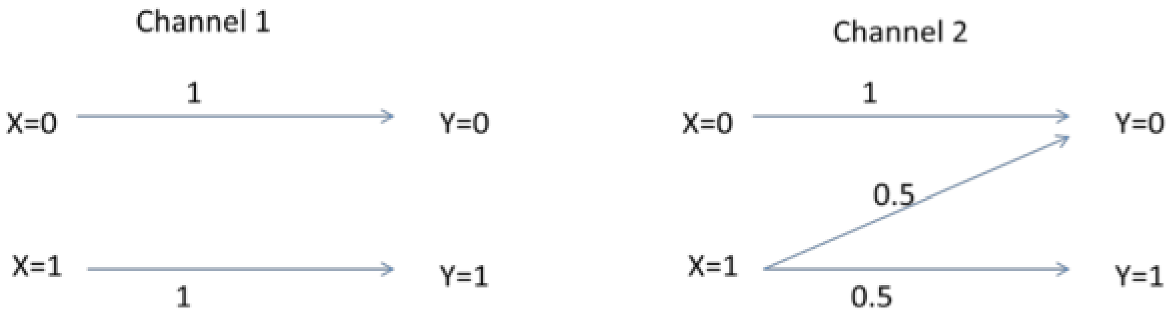
3. Find the Lempel-Ziv source code for the binary source sequence
000101010010011010100001010111100011011000011101011
Symbol alphabet is {0, 1}.
Please show all steps of your work clearly.

0,0|0,1|01,0|10,0|100,1|101,0|100,0|010,1|0111,1|0001,1|0110,0|0011,1|0101,1
Ø0, Ø1, 10, 20, 41, 50, 40, 31, 71, 11, 60, 31, 51
Lempel-Ziv source code is
0100 1010 1101 0100 0011 0010 1101 000 0110 11

4. Show that {01, 100, 101, 1110, 1111, 0011, 0001} cannot be a Huffman Code for any source probability distribution.

For this encoding, it clearly shows that not all symbols are used at the bottom of the Huffman Encoding tree, i.e. 0000, 0010, 1010, 1011, 1100, 1101. This means that the total probability of this encoding WILL NOT be 1.

5. Channels 1 and 2 are shown in the following. The source is characterized by $P(X=0)=q$.



Find the capacity of Channel 1 and 2 as a function of q. What values of q will maximise I(X;Y) of Channel 1 and Channel 2?

For simplicity, we denote $\log_2$ as $\log$.

$$I(X;Y)=H(X)-H(X|Y)=H(Y)-H(Y|X)$$

$$H(X)=\sum_{i=1}^{\boldsymbol{n}}P(x_i)\log\frac{1}{P(x_i)}\ bits$$

$$H(X|Y)=-\sum_{x\epsilon Y}\sum_{y\epsilon X}P(X=x|Y=y)P(Y=y)\log P(X=x|Y=y)$$

Channel 1 is a *noiseless binary channel*.
Since Channel 1 is a noiseless binary channel,

$$I(X;Y)=H(X)-H(X|Y)=H(X)$$

$$H(X)=\sum_{i=1}^{\boldsymbol{n}}P(x_i)\log\frac{1}{P(x_i)}$$

$$=q\log\frac{1}{q}-(1-q)\log\frac{1}{1-q}$$

$$=-q\log q+(q-1)\log(1-q)$$

$$=I(X;Y)$$

$$C=\max_{P(x)}I(X;Y)$$

$$=\max_{P(x)}(-q\log q+(q-1)\log(1-q))$$

To maximise $I(X;Y)$ of Channel 1, take the derivative of C and set it to 0.

$$\max_{P(x)}I(X;Y)=0$$

$$\frac{d}{dq}(-q\log q+(q-1)\log(1-q))=0$$

$$\frac{1}{\log 2}\frac{d}{dq}\left(-q\ln q + (q-1)\ln(1-q)\right) = 0$$

$$\ln(1-q) - \ln q \ = 0$$

$$\frac{1-q}{q} = 0$$

$$q = \frac{1}{2}$$

Thus, $I(X;Y)$ is maximised at $q = \frac{1}{2}$.

Channel 2 is a *Z-Channel.*

$$H(Y|X) = -\sum_{y\epsilon X}\sum_{x\epsilon Y} P(Y=y|X=x)P(X=x)\log P(Y=y|X=x)$$

$$= -P(X=0)P(Y=0|X=0)\log(Y=0|X=0)$$
$$-P(X=1)P(Y=0|X=1)\log(Y=0|X=1)$$
$$-P(X=1)P(Y=1|X=1)\log(Y=1|X=1)$$

$$= -\frac{1-q}{2}\log\frac{1}{2} - \frac{1-q}{2}\log\frac{1}{2}$$

$$= 1-q$$

The probability mass function for $P(Y)$ are as follow:

$$P(Y=0) = P(X=0)P(Y=0|X=0) + P(X=1)P(Y=0|X=1)$$

$$= q + \frac{(1-q)}{2}$$

$$= \frac{1+q}{2}$$

$$P(Y=1) = P(X=1)P(Y=1|X=1)$$

$$= \frac{1-q}{2}$$

Therefore,

$$H(Y) = \sum_{i=1}^{\boldsymbol{n}} P(y_i)\log\frac{1}{P(y_i)}$$

$$= \frac{1+q}{2}\log\frac{1}{\frac{1+q}{2}} + \frac{1-q}{2}\log\frac{1}{\frac{1-q}{2}}$$

$$= \frac{1+q}{2}\left(1-\log(1+q)\right) + \frac{1-q}{2}\left(1-\log(1-q)\right)$$

$$= -\frac{1+q}{2}\log(1+q) - \frac{1-q}{2}\log(1-q) + 1$$

Then,

$$I(X;Y) = H(Y) - H(Y|X)$$

$$= \left(-\frac{1+q}{2}\log(1+q) - \frac{1-q}{2}\log(1-q) + 1\right) - (1-q)$$

$$C = \max_{P(x)} I(X;Y)$$

$$= \max_{P(x)} \left(-\frac{1+q}{2}\log(1+q) - \frac{1-q}{2}\log(1-q) + 1\right) - (1-q)$$

To maximise $I(X;Y)$ of Channel 2, take the derivative of C and set it to 0.

$$\max_{P(x)} I(X;Y) = 0$$

$$\frac{d}{dq}\left(\left(-\frac{1+q}{2}\log(1+q) - \frac{1-q}{2}\log(1-q) + 1\right) - (1-q)\right) = 0$$

$$\frac{1}{\ln 2}\left(-\frac{\ln(1+q)}{2} + \frac{\ln(1-q)}{2}\right) + 1 = 0$$

$$\log\frac{1-q}{1+q} + 2 = 0$$

$$\frac{1-q}{1+q} = \frac{1}{4}$$

$$q = \frac{3}{5}$$

Thus, $I(X;Y)$ is maximised at $q = \frac{3}{5}$.

6. **A binary PAM communication system employs rectangular pulses of duration $T_b$and amplitude$\pm A$ to transmite digital information at $R = 10^5$ bits/sec. If the power spectral density of the additive white Gaussian noise is $\frac{N_0}{2}$, where $N_0 = 10^{-2}$ W/Hz, determine the value of A that is required to achieve an error probability of $P_b = 10^{-6}$.**

We have a transmission rate of $R = 10^5$ bit/sec. So, the transmission time per bit, i.e. rectangular pulse duration is $T_b = \frac{1}{R} = 10^{-5}$ sec/bit.
Let $s_0(t)$ and $s_1(t)$ be the two symbols of binary PAM.
The energy of a symbol for binary PAM is given by

$$\varepsilon_b = \int_{-\infty}^{+\infty} |s_0(t)|^2\,dt = \int_{-\infty}^{+\infty} |s_1(t)|^2\,dt$$

$$= \int_0^{T_b} A^2\,dt$$

$$= A^2 T_b$$

$$= 10^{-5}\times A^2$$

Probability of error for binary PAM is given by

$$P_b = Q\left(\sqrt{\frac{2\varepsilon_b}{N_0}}\right)$$

$$10^{-6} = Q\left(\sqrt{\frac{2A^2\times 10^{-5}}{10^{-2}}}\right)$$

With reference to *Table of the Q Funct*ion from *Fundamentals of Communication Systems*, we have $Q(4.7)\approx 10^{-6}$.
Therefore,

$$Q(4.7) = Q\left(\sqrt{\frac{2A^2\times 10^{-5}}{10^{-2}}}\right)$$

$$4.7 = \sqrt{\frac{2A^2\times 10^{-5}}{10^{-2}}}$$

$$22.09 = 2\times 10^{-3}\times A^2$$

$$A = 105$$

7. In a binary antipodal signalling scheme, the signals are given by

$$s_1(t) = -s_2(t) = \begin{cases} \frac{2A}{T}t, & 0\le t<\frac{T}{2} \\ 2A\left(1-\frac{t}{T}\right), & \frac{T}{2}\le t<T \\ 0, & oterwise \end{cases}$$

The channel is AWGN and the power spectral density of the noise is $\frac{N_0}{2}$. The two signals have prior probabilities of p and $1-p$.

a) Determine the energy consumed for transmission of a single bit, ε_b.

$$\varepsilon_b = \int_{-\infty}^{+\infty} |s_1(t)|^2\,dt = \int_{-\infty}^{+\infty} |s_2(t)|^2\,dt$$

$$= \int_0^{\frac{T}{2}} \left(\frac{2A}{T}t\right)^2 dt + \int_{\frac{T}{2}}^{T} \left(2A(1-\frac{t}{T})\right)^2 dt$$

$$= \int_0^{\frac{T}{2}} \frac{4A^2}{T^2}t^2\,dt + \int_{\frac{T}{2}}^{T} \left(2A-\frac{2A}{T}t\right)^2 dt$$

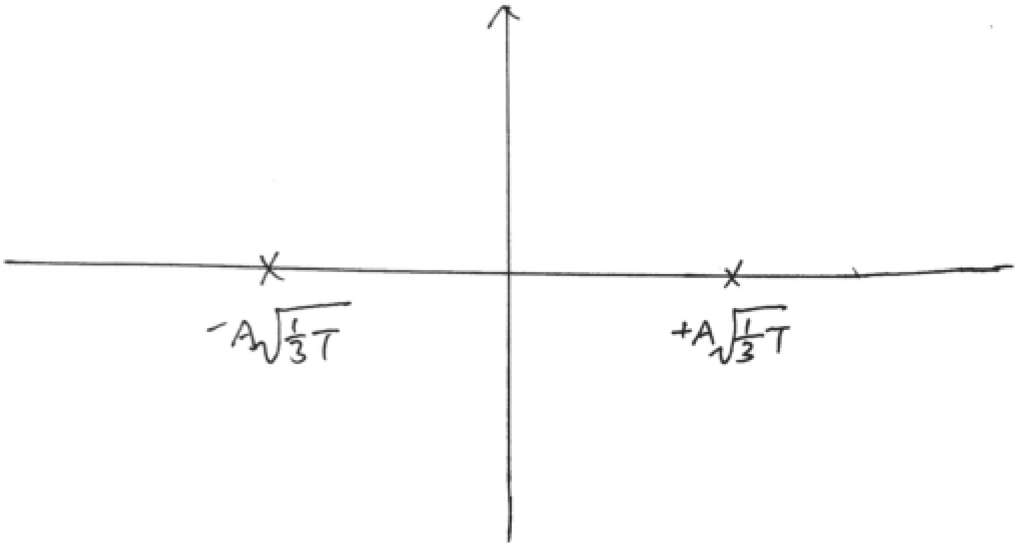
$$= \frac{4A^2}{3T^2}\times\left(\frac{T}{2}\right)^3 + \int_{\frac{T}{2}}^{T} \left(4A^2-\frac{8A^2}{T}t+\frac{4A^2}{T^2}t^2\right)dt$$

$$= \frac{4A^2}{3T^2} \times \frac{T^3}{8} + \left(4A^2 \times T - 4A^2 \times T + \frac{4}{3}A^2 \times T\right) - \left(4A^2 \times \frac{T}{2} - 8A^2 \times \left(\frac{T}{2}\right)^2 + \frac{4}{3}A^2 \times \left(\frac{T^3}{8}\right)\right)$$

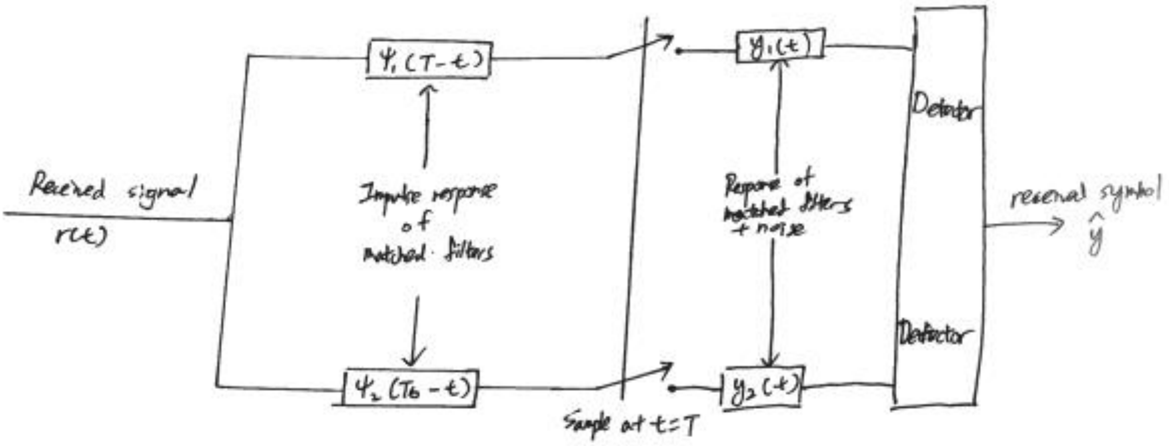
$$= \frac{A^2T}{6} + \frac{4}{3}A^2T - A^2T - \frac{A^2T}{6}$$

$$= \frac{1}{3}A^2T$$

b) Plot the constellation diagram for this system.



c) Determine the matched-filter based structure of the optimal receiver.



d) Determine the detection threshold τ_h as a function of A, T, N_0, p.

For binary antipodal signals, the average probability of error as a function of threshold τ is

$$P(\tau) = P(s_1)\int_{-\infty}^{\tau} f(r|S_1)dr + P(s_2)\int_{\tau}^{+\infty} f(r|s_2)dr$$

To determine τ_h, which minimises the average probability of error, we differentiate $P(\tau)$ with respect to τ and setting the derivative to zero. We then obtain

$$P(s_1)f(r|s_1) - P(s_2)f(r|s_2) = 0$$

$$\frac{f(r|s_1)}{f(r|s_2)} = \frac{P(s_2)}{P(s_1)}$$

since $s_1 = \sqrt{\varepsilon_b}$ and $s_2 = -\sqrt{\varepsilon_b}$, we have

$$e^{-\frac{\left(\tau_h-\sqrt{\varepsilon_b}\right)^2}{N_0}} e^{-\frac{\left(\tau_h+\sqrt{\varepsilon_b}\right)^2}{N_0}} = \frac{P(s_2)}{P(s_1)}$$

$$e^{\frac{4\tau_h\sqrt{\varepsilon_b}}{N_0}} = \frac{P(s_2)}{P(s_1)}$$

Taking natural logarithm, it is simplified to

$$\frac{4\tau_h\sqrt{\varepsilon_b}}{N_0} = \ln\frac{\mathrm{P(s_2)}}{P(s_1)}$$

$$\tau_h = \frac{N_0}{4\sqrt{\varepsilon_b}}\ln\frac{\mathrm{P(s_2)}}{P(s_1)}$$

$$= \frac{N_0}{4\sqrt{\frac{1}{3}A^2T}}\ln\frac{1-\mathrm{p}}{p}$$

$$= \frac{N_0}{4A}\sqrt{\frac{3}{T}}\ln\frac{1-\mathrm{p}}{p}$$

e) Determine an expression for the error probability.

For binary antipodal signalling scheme,

$$P_b = \frac{1}{2}\left(P(e|s_0) + P(e|s_1)\right)$$

where $P(e|s_0) = P(e|s_1)$ due to symmetry of the system, i.e. error rate for s_0, s_1 are equally probable.

So,

$$P(e|s_0) = P(e|s_1) = P(r < 0 \mid s_1)$$

$$= \int_{-\infty}^{0} f_R(r|s_1)dr$$

$$= \int_{-\infty}^{0} \frac{1}{\sqrt{\pi N_0}} e^{-\frac{\left(r-\sqrt{\varepsilon_b}\right)^2}{N_0}} dr$$

$$= \frac{1}{\sqrt{\pi}}\int_{\sqrt{\frac{2\varepsilon_b}{N_0}}}^{\infty} e^{-\frac{x^2}{2}}dx$$

$$= Q\left(\sqrt{\frac{2\varepsilon_b}{N_0}}\right)$$

$$= Q\left(\sqrt{\frac{2A^2T}{N_0}}\right)$$

8.

a) Consider a transposition encryption system with the encryption key of "KARMA". Let assume that the input plaintext to the system is the following text:

"TRANSPOSTION CIPHER CHANGES THE ORDER OF THE LETTERS"

Determine the equivalent cipher text for the above plaintext, neglecting the spaces between subsequent words in the plaintext. You will need to produce the transposition table and the cipher-text in your answer, all in capital letters.

K	**A**	**R**	**M**	**A**
3	**1**	**5**	**4**	**2**
T	R	A	N	S
P	O	S	T	I
O	N	C	I	P
H	E	R	C	H
A	N	G	E	S
T	H	E	O	R
D	E	R	O	F
T	H	E	L	E
T	T	E	R	S

Cipher text: RONENHEHTSIPHSRFESTPOHATDTTNTICEOOLRASCRGEREE

b) Briefly describe the 3 main pieces of information that an adversary needs to carry out a brute force attack against a symmetric encryption system.

An adversary would need to know some plaintext, matched cipher text and number of keys to carry out a brute force attack against a symmetric encryption system.

c) Consider a brute force attack scenario, where the adversary uses a computer that can examine 10^{12} key combinations every second. How many hours will be required to break a DES encryption system with 56-bit key and 3DES encryption system with a 112-bit key?

Let:

t_1, t_2be the time required to break DES encryption system with 56-bit key and 3DES encryption system with 112-bit key respectively.

For DES 56-bit key,

$$t_1 = \frac{2^{56}}{10^{12}} \times \frac{1}{3600}$$

$$= 20.0\ hours$$

For 3DES 112-bit key,

$$t_2 = \frac{2^{112}}{10^{12}} \times \frac{1}{3600}$$

$$= 9.45 \times 10^{22}\ hours$$

9. **Consider a CSMA/CD network running at 1Gbps over a 1km cable. The signal speed in the cable is 200,000 km/sec. Determine the minimum frame size for this system.**

Let τ be the round-trip delay, b be the bandwidth and f be the minimum number of frame size.

$$f \geq \tau b$$

$$\geq \frac{1 \times 2}{200000} \times 10^9$$

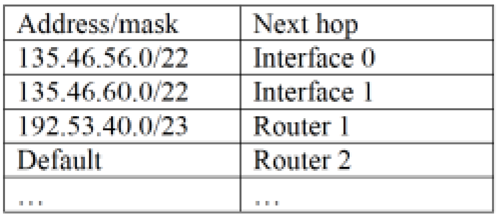
$$\geq 10000$$

Taking the nearest number with power of 8,

$$f = 10000\ bits$$

$$= 1250\ bytes$$

10. **A router has the following CIDR entries in its routing table:**



Address/mask	Next hop
135.46.56.0/22	Interface 0
135.46.60.0/22	Interface 1
192.53.40.0/23	Router 1
Default	Router 2
…	…

For each of the following IP addresses, what does the router do if a packet with that address arrives at the router?

When a packet arrives at a router, the routing table Is scanned to determine if the destination lies within the prefix. It uses the longest prefix if multiple entries match.

a) **135.46.63.10**
The IP address lies in Interface 1, where the range is within 135.46.60.0 – 135.46.63.255.
The packet will arrive at Interface 1.

b) **135.46.57.14**
The IP address lies in Interface 0, where the range is within 135.46.56.0 – 135.46.59.255.
The packet will arrive at Interface 0.

c) **135.46.52.2**
The IP address is out of range of any given IP addresses. Thus, it will go to the default address.
The packet will arrive at Router 2.

d) **192.53.40.7**
The IP address lies in Router 1, where the range is within 192.53.40.0 – 192.53.41.255.
The packet will arrive at Router 1.

e) **191.53.56.7**
The IP address is out of range of any given IP addresses. Thus, it will go to the default address.
The packet will arrive at Router 2.