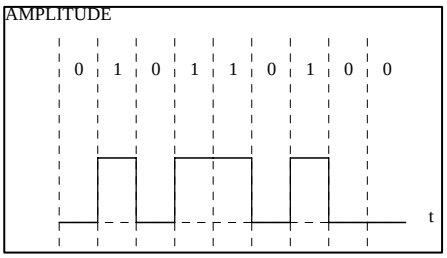
2011 Past Paper –Question 4

(a) Baseband transmission is typically identified when the transmission has a large percentage of their spectrum near DC. It is common for baseband signals to be used in communication systems such as Ethernet for example. Human interference on the transmission can be reduced or eliminated by careful engineering whilst natural phenomena produce noise, presenting a fundamental limit to system performance.

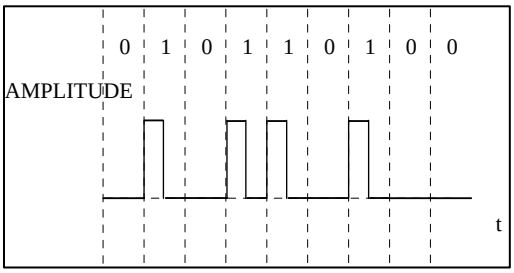
Conversely, for modulated transmission, the baseband signal is used to modulate a higher frequency carrier wave that is more suited to the transmission channel, potentially allowing for higher performance at the cost of added complexity of a modulator and demodulator at the transmitter and receiver respectively. 6

(b) Full marks for any two of the following four diagrams with the correct identifications

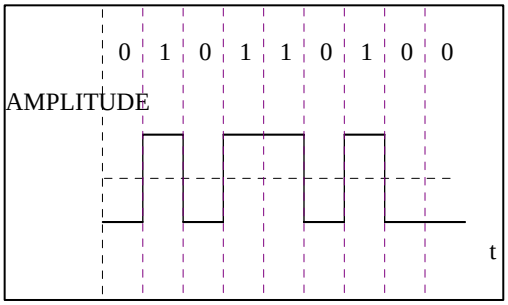
Unipolar NRZ



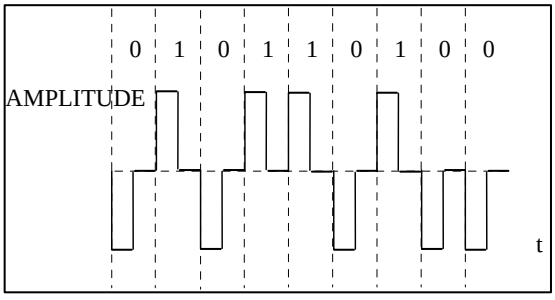
Unipolar RZ 6



Polar NRZ



Unipolar RZ



(c) ASK behaves like baseband OOK for error rate purposes and is particularly susceptible to noise because information is conveyed by amplitude. For a carrier peak amplitude of A_c, coherent transmission with noise power σ

$$P_e = \frac{1}{2} erfc\left(\frac{A_c}{2\sqrt{2}\sigma}\right)$$

FSK and PSK have a carrier present at all times producing

$P_e = \frac{1}{2} erfc\left(\frac{A_c}{2\sigma}\right)$ and $P_e = \frac{1}{2} erfc\left(\frac{A_c}{\sqrt{2}\sigma}\right)$ respectively.

In both cases, the ratio A_c/σ is divided by a smaller number so the probability of error will be less as the SNR is increased. FSK spectrum is like 2 ASK signals spaced by the frequency deviation, PSK has same bandwidth as ASK.

ASK bandwidth is $2B_T$ for bit rate B_T
FSK bandwidth is $2B_T + \Delta f$
PSK bandwidth is $2B_T$
So PSK becomes attractive when bandwidth is limited.

(d) From the question:- $A_c = 5$ and $\sigma = 0.7$ and using the approximation $erfc(x) \approx \exp\left(-x^2\right)/x\sqrt{\pi}$, the probability of error for each can be determined as:-

$$P_e(ASK) = \frac{1}{2} erfc\left[\frac{A_c}{2\sqrt{2}\sigma}\right] = \frac{1}{2} erfc\left[\frac{5}{2\sqrt{2}\times 0.7}\right] = \frac{1}{2} erfc[2.53]$$

$$\approx \frac{1}{2\times 2.53\sqrt{\pi}} \exp\left(-2.53^2\right) \approx 1.85\times 10^{-4}$$

$$P_e(FSK) = \frac{1}{2} erfc\left[\frac{A_c}{2\sigma}\right] = \frac{1}{2} erfc\left[\frac{5}{2\times 0.7}\right] = \frac{1}{2} erfc[3.57]$$

$$\approx \frac{1}{2\times 3.57\sqrt{\pi}} \exp\left(-3.57^2\right) \approx 2.31\times 10^{-7}$$

$$P_e(ASK) = \frac{1}{2} erfc\left[\frac{A_c}{\sqrt{2}\sigma}\right] = \frac{1}{2} erfc\left[\frac{5}{\sqrt{2}\times 0.7}\right] = \frac{1}{2} erfc[5.05]$$

$$\approx \frac{1}{2\times 5.05\sqrt{\pi}} \exp\left(-5.05^2\right) \approx 4.69\times 10^{-13}$$

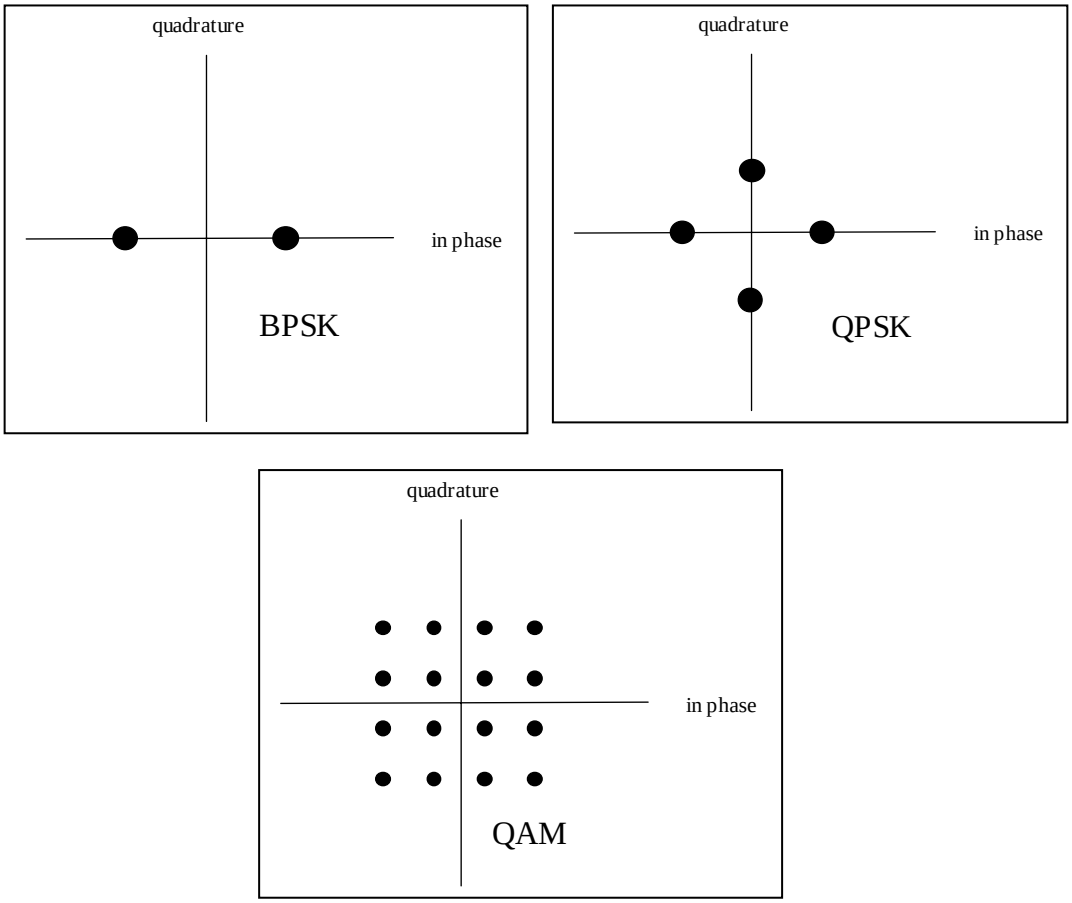
Therefore the number of errors per second at 1Mbps is:

$$ASK: \left(1.85\times10^{-4}\right)\times\left(1\times10^{6}\right)=185$$
$$FSK: \left(2.31\times10^{-7}\right)\times\left(1\times10^{6}\right)=0.231$$
$$PSK: \left(4.69\times10^{-13}\right)\times\left(1\times10^{6}\right)=4.96\times10^{-7}$$

Thus the time between errors (in seconds) is

$$ASK: (185)^{-1}=5.4\times10^{-3}$$
$$FSK: (0.231)^{-1}=4.3$$
$$PSK: \left(4.96\times10^{-7}\right)^{-1}=2\times10^{6}$$

(e) If we have B Hz of usable bandwidth the data rate may be increased by transmitting more information per symbol using multi-level signalling. For example in ASK if we use 4 amplitude levels instead of 2 then each symbol represents 2 bits of information and the data rate becomes 2B bits/s. Increasing from 2 to M levels increases our data rate to $\log_2 M \times B$ bits/s which enables higher data rates without the requirement for more bandwidth. The possible phases and amplitudes may be neatly represented on constellation diagrams as shown



2011 Past Paper –Question 5

(a) In algebraic coding, redundant parity bits are added to a message to aid the process of error correction. The presence of such redundant bits increases the number of possible bit sequences that may be transmitted thus allowing there to be an increased distance (in terms of differences in bit positions) between the messages used. At the receiver, the message that is most similar to that received is used and this allows several errors to occur before the received message becomes closer to another message other than that which was sent.

(b) Rather than sending 0 or 1 to represent the data, we use 000 and 111. This means that a message will only be erroneously decoded if two or three bits are corrupted. If only one error occurs, the received message is still closest to the correct one. For example, 010 will be interpreted as 000 assuming that the middle bit is in error. The addition of two extra bits for this limited amount of error correction is not efficient since it requires three times the data rate compared with the uncoded data.

(c) Given a binary message, even (odd) parity indicates that the number of 1s in the message is even (odd). The utilisation of parity checks on combinations of the bits from a block of data enables more powerful codes to be realised since more use is being made of the message bits than just their repetition. Linear algebraic codes are formed from the product of a generator matrix with the message. At the receiver, the product of the received message and a parity check matrix is formed. The result of the product produces the information required to find and correct errors.

(d)

i. The number of code words is $2^4 = 16$ and the code rate is $\frac{4}{7}$

ii. The parity check matrix is formed (as provided)

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Thus, the parity check matrix is:

$$\mathbf{H}^{T}=\begin{bmatrix}1&1&1\\0&1&1\\1&0&1\\1&1&0\\1&0&0\\0&1&0\\0&0&1\end{bmatrix} \quad \text{and/or} \quad \mathbf{H}=\begin{bmatrix}1&0&1&1&1&0&0\\1&1&0&1&0&1&0\\1&1&1&0&0&0&1\end{bmatrix}$$

The Syndrome is therefore, by using **R** (as provided):

$$\mathbf{S}=\mathbf{H.R}=\begin{bmatrix}1&0&1&1&1&0&0\\1&1&0&1&0&1&0\\1&1&1&0&0&0&1\end{bmatrix}\begin{bmatrix}1\\1\\1\\0\\0\\1\\0\end{bmatrix}=\begin{bmatrix}0\\1\\1\end{bmatrix}$$

iii. The syndrome should be zero for a correct message to conform to the parity process.

The decoding process is represented as: **S = H.R = H.(T⊕E) = H.T ⊕ H.E**

Since the product of the correct message and **H** is zero (**S=H.E)**, if a single error occurs, the product **H.E**

$$\begin{bmatrix}1&0&1&1&1&0&0\\1&1&0&1&0&1&0\\1&1&1&0&0&0&1\end{bmatrix}\begin{bmatrix}E_1\\E_2\\E_3\\E_4\\E_5\\E_6\\E_7\end{bmatrix}=\begin{bmatrix}0\\1\\1\end{bmatrix}$$

will copy one column of **H** into the syndrome because only one of the E_n values will be one.

In this case, the syndrome is identical to the second column in **R** so bit two must be incorrect and the message should be:

$$\mathbf{R}^{T}=\begin{bmatrix}1&0&1&0&0&1&0\end{bmatrix}$$

2011 Past Paper –Question 6

(a) A code is said to be a prefix code, if none of the codewords is a prefix of any of the others. A code is uniquely decidable (UD) is any output string is the image of a most one input message.

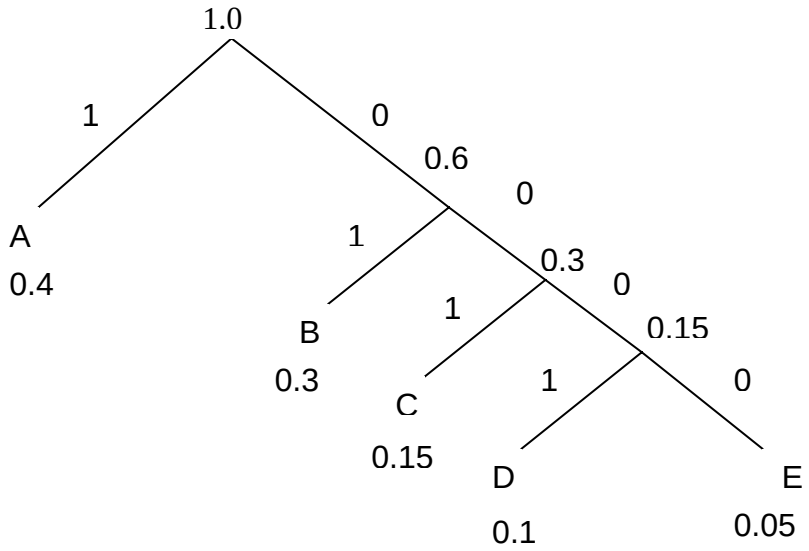
(b) Using the probabilities provided in the question

$$P(A) = 0.4\ ,\ P(B) = 0.3,\ P(C) = 0.15\ ,\ P(D) = 0.1,\ P(E) = 0.05$$

(i) Produce a clear table as in the lecture similar to:

Initial Probabilities				
A 0.4 B 0.3 C 0.15 D 0.1 E 0.05				
Combine the lowest two				
A 0.4 B 0.3 C 0.15 D 0.1 E 0.05	A 0.4 B 0.3 C 0.15 DE 0.15			
Combine the lowest two				
A 0.4 B 0.3 C 0.15 D 0.1 E 0.05	A 0.4 B 0.3 C 0.15 DE 0.15	A 0.4 B 0.3 CDE 0.3		
Combine the lowest two				
A 0.4 B 0.3 C 0.15 D 0.1 E 0.05	A 0.4 B 0.3 C 0.15 DE 0.15	A 0.4 B 0.3 CDE 0.3	A 0.4 BCDE 0.6	
Combine the lowest two				
A 0.4 B 0.3 C 0.15 D 0.1 E 0.05	A 0.4 B 0.3 C 0.15 DE 0.15	A 0.4 B 0.3 CDE 0.3	A 0.4 BCDE 0.6	ABCDE 1

Subsequently, the Huffman tree diagram can be easily shown to be:



Such that Huffman code should read:

$A \mapsto 1$		$A \mapsto 0$
$B \mapsto 01$		$B \mapsto 10$
$C \mapsto 001$	SWAPPING 0 AND 1	$C \mapsto 110$
$D \mapsto 0001$		$D \mapsto 1110$
$E \mapsto 0000$		$E \mapsto 1111$

(ii) The entropy of the DMS is given by:

$$\begin{aligned} H(X) &= -0.4\log_2 0.4 - 0.3\log_2 0.3 - 0.15\log_2 0.15 \\ &\quad - 0.1\log_2 0.1 - 0.05\log_2 0.05 \\ &= 2.0087 \end{aligned}$$

(iii) The code length is given by:

$$\begin{aligned} l &= 0.4 + 0.3\times 2 + 0.3\times 3 + 0.15\times 4 + 0.05\times 4 \\ &= 2.05 \end{aligned}$$

Where is can be seen that the code length is greater than the entropy and so not a Shannon optimum code.

(iv) The compression ratio is given by

$$\rho = \frac{l}{\log_2(5)} = \frac{2.05}{2.3219} = 0.88$$

(c) The aim of compression is to reduce the amount of transmitted/stored data. This is typically carried out by looking for patterns within the data and using various methods to replace or remove such pattern with a smaller number of data points. Conversely, a good encryption scheme will produce a data set that has no decipherable pattern. Attempting to compress an encrypted data set will result in virtually no compression such that one has to compress the data before encryption.

(d) The RSA system relies on the intractability of factorisation compared with the ease of finding large prime numbers. Each participant creates his keys as follows:

1. Select at random two large primes.

2. Compute $n = qr$

3. Select a small odd integer *p* relatively prime to $\phi(n) = (q-1)(r-1)$.

4. Compute *s*, the multiplicative inverse of p mod $\phi(n)$.

5. Publish (*p*,*n*) as public key.

6. Keep secret (*s*,*n*) as secret key.

Messages *M* are encrypted by $C = M^p \bmod n$.

Ciphertexts *C* are decrypted by $M = C^S \bmod n$.

To obtain the secret key from the public one the cryptanalyst would need to factor *n* to obtain *q* and *r* and hence $\phi(n)$.