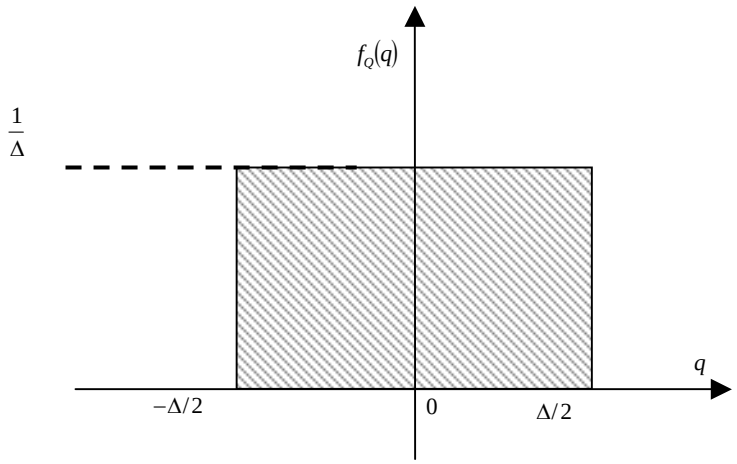
2008 Past Paper –Question 4

(a) The transformation of an analogue input signal to its digital approximation requires mapping to a set of digital levels, taking the closest one to the signal as its value. This approximation process is known as quantisation. The error in the approximation of the signal by the levels is by default uniformly distributed between $-\Delta/2$ and $\Delta/2$ for a level spacing of Δ. Since the signal is not known *a priori*, the error is a random variable that is known as the quantisation noise.

(b) For uniform sampling, the error is distributed as shown



$$f_Q(q) = \begin{cases} \dfrac{1}{\Delta} & -\dfrac{\Delta}{2} < q < \dfrac{\Delta}{2} \\ 0 & \text{otherwise} \end{cases}.$$

$$E[q] = \frac{1}{\Delta}\int_{-\frac{\Delta}{2}}^{\frac{\Delta}{2}} x\,dx = \frac{1}{\Delta}\frac{x^2}{2}\Big|_{-\frac{\Delta}{2}}^{\frac{\Delta}{2}} = 0$$

As the mean is zero

$$\sigma_Q^2 = E\left[x^2\right] = \frac{1}{\Delta}\int_{-\frac{\Delta}{2}}^{\frac{\Delta}{2}} x^2 dx = \frac{1}{\Delta}\frac{x^3}{3}\Big|_{-\frac{\Delta}{2}}^{\frac{\Delta}{2}} = \frac{1}{\Delta}\left\{\frac{1}{3}\frac{\Delta^3}{8} + \frac{1}{3}\frac{\Delta^3}{8}\right\} = \frac{\Delta^2}{12}$$

(c) The sqer is the ratio of the mean squared signal level to the mean squared quantisation noise ratio, usually given in dB.

Here, the signal pdf is symmetric about zero and thus the signal is zero mean.

We need to find the expected value of v^2 to give the mean square value but first need the expression for the pdf.

This is easily found to be

$$p(v)=\begin{cases}1/v_m(1+v/v_m) & -v_m<v<0\\ 1/v_m(1-v/v_m) & 0<v<v_m\\ 0 & \text{otherwise}\end{cases}$$

So

$$E[v^2]=\frac{1}{v_m}\int_0^{v_m}v^2(1-v/v_m)dv+\frac{1}{v_m}\int_{-v_m}^{0}v^2(1+v/v_m)dv$$

$$=\frac{1}{v_m}\left\{\frac{v^3}{3}-\frac{v^4}{4v_m}\right\}_0^{v_m}+\frac{1}{v_m}\left\{\frac{v^3}{3}+\frac{v^4}{4v_m}\right\}_{-v_m}^{0}$$

$$=\frac{1}{v_m}\left\{\frac{{v_m}^3}{3}-\frac{{v_m}^4}{4v_m}\right\}-\frac{1}{v_m}\left\{\frac{-{v_m}^3}{3}+\frac{{v_m}^4}{4v_m}\right\}$$

$$E[v^2]=v_m^2\left\{\frac{1}{3}-\frac{1}{4}\right\}-v_m^2\left\{\frac{-1}{3}+\frac{1}{4}\right\}$$

$$=v_m^2\left\{\frac{2}{3}-\frac{1}{2}\right\}=\frac{v_m^2}{6}$$

For a linear quantiser with N levels and steps of Δ, $v_m=\frac{N\Delta}{2}$

$$\text{sqer}=\frac{v_m^2/6}{(\Delta)^2/12}=\frac{N^2(\Delta)^2/24}{(\Delta)^2/12}=\frac{N^2}{2}$$

(d) The sqer is 50 dB when

$$10\log_{10}\left(\frac{N^2}{2}\right) = 50$$

$$20\log_{10}\left(\frac{N}{\sqrt{2}}\right) = 50$$

$$N = \sqrt{2}\times 10^{2.5}$$

$$= 447.2$$

Since $2^9 = 512$, 9 bits will suffice making the minimum bit rate $9\times 20 = 180$ kbps because we must sample at the Nyquist rate of 20 ksamples per second.

2008 Past Paper –Question 5

(a) The noise remains Gaussian because the filter is linear but with a changed variance.

However, its power spectral density is modified.

At the output, the PSD is

$$G_o(f) = |H(f)|^2 G_i(f)$$

(b) The pulse given is White Gaussian Noise of PSD $N_0/2$ V^2/Hz passed through a low pass RC network.

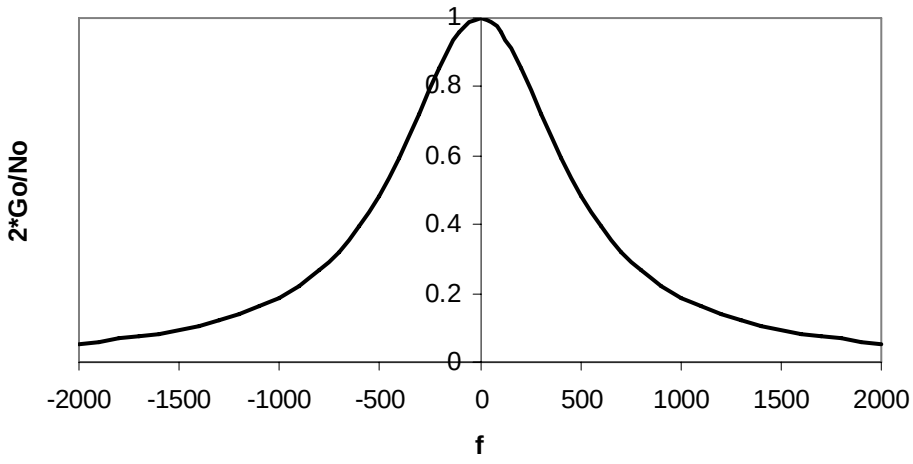
$$H(f) = \frac{1/j2\pi fC}{R + 1/j2\pi fC} = \frac{1}{1 + j2\pi fCR}$$

$$|H(f)|^2 = \frac{1}{1 + (2\pi fCR)^2} = \frac{1}{1 + \left(\frac{f}{f_0}\right)^2} \quad f_0 = 1/2\pi CR$$

So

$$G_o(f) = |H(f)|^2 G_i(f)$$
$$= \frac{N_0}{2} \frac{1}{1 + \left(\frac{f}{f_0}\right)^2}$$

which we can sketch for $N_0/2=10^{-8}$ and $f_0=1/(2\pi\times10^{-9}\times330) = 482.3$ kHz



$$P_{OUT} = \int_{-\infty}^{\infty} G_o(f)df$$
$$= \int_{-\infty}^{\infty} \frac{N_0}{2} \frac{1}{1+\left(f/f_0\right)^2} df$$
$$\text{subst } f = f_0 \tan\theta df = f_0 \sec^2\theta d\theta$$
$$P_{OUT} = \frac{N_0}{2} \int_{-\pi/2}^{\pi/2} \frac{f_0 \sec^2\theta}{1+\tan^2\theta} d\theta$$

$$P_{OUT} = \frac{N_0}{2} \int_{-\pi/2}^{\pi/2} f_0 d\theta = \frac{N_0 f_0 \pi}{2}$$

Putting in the expression for f_0 gives us

$$P_{OUT} = \frac{N_0 \pi \left(\frac{1}{2\pi CR}\right)}{2} = \frac{N_0}{4CR} = \frac{N_0/2}{2CR}$$
$$= \frac{10^{-8}}{2\times 10^{-9} \times 330} = 15.2\text{mW}$$

(c) The signal at the point of comparison with the noise is

$$p_o(T) = \int_{-\infty}^{\infty} P(f)H(f)e^{j2\pi fT} df$$

We need $\left|\int_{-\infty}^{\infty} P(f)H(f)e^{j2\pi fT} df\right|^2$ but here it is much easier to realise that the pulse will be an exponential rise since we are charging a capacitor. At the end of the bit period the output of the filter will be $1.5\left(1-e^{-T/CR}\right)$. At 2Mbits^{-1}

T = 1/(2×10^6), T/CR = 1/(2×10^6×10^{-9}×330) = 1.52, so the signal power is $\left[1.5\left(1-e^{-1.52}\right)\right]^2 = 1.373$ W.

Thus SNR = 1.373/0.0152 = 90.33 and

$$P_e = \frac{1}{2}\text{erfc}\left[\sqrt{\frac{SNR}{8}}\right] = \frac{1}{2}\text{erfc}[3.36] \approx \frac{1}{2}\frac{e^{-3.36^2}}{3.36\sqrt{\pi}} = 1.05\times10^{-6}$$

(d) Matched filter SNR is

$$\frac{2}{N_0}\int_{-\infty}^{\infty} p^2(t)dt = \frac{2}{N_0}\int_0^T 1.5^2\,dt = \frac{1}{10^{-8}}\frac{2.25}{2\times10^6} = 112.5$$

So penalty SNR(matched)/SNR(CR) = 112.5/90.33 = 1.245 =0.95 dB, so a sub-optimal filter may have a performance very close to the matched filter if the bandwidth is carefully selected.

2008 Past Paper –Question 6

(a) Additive ciphers use an encrypting transform that is just mod *m* addition, where *m* is the modulus of the cipher.

So for a key k_+ the transform is $a \mapsto a +_m k_+$ with corresponding decrypting transform $a \mapsto a -_m k_+$.

Multiplicative ciphers use the encrypting transformation $a \mapsto a \times_m k$. This is multiplication modulo m and the decrypting transformation is $a \mapsto a \times_m k^{-1}$, where k^{-1} is the multiplicative inverse of k, that is $k \times_m k^{-1} = k^{-1} \times_m k = 1$. 6

We can combine an additive and a multiplicative cipher to obtain an affine cipher. An affine cipher comprises multiplication by one key $(k_\times)$, and then addition of a second key (k_+). The pair is written $(k_\times, k_+)$.

Encryption: $a \mapsto a \times_m k_\times +_m k_+$; decryption: $b \mapsto (b -_m k_+) \times_m k_\times^{-1}$.

(b) Additive cipher keys must be $0 < k_+ < m$, where m is the modulus. For multiplicative ciphers the key must, in addition, be coprime or ***relatively prime*** to (have no common factors with) the modulus. Keys will then all have inverses, enabling a unique encoding and make decoding possible. In an affine cipher, the additive key (k_+) is constrained as the key to an additive cipher and the multiplicative key $(k_\times)$ as the key to a multiplicative cipher.

Using mod 10, all keys should be > 0 and < 10 so k_+ may be

1 2 3 4 5 6 7 8 9

Furthermore, the $k_\times$ keys may not be even (since two is a factor of 10) also 5 fails similarly. This leaves the numbers

1 3 7 9

although 1 would not do a good job in hiding the plaintext, it is permissible.

(c) The use of the special symbol makes this cipher much easier to crack if it is assumed that it will be the most common occurrence because of its use. The system is modulo 27 because of the extra symbol.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Φ
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

The table shows the letters and their numerical equivalent mod 27.

For the message *GWVVYGJVKLG* it is reasonable to assume that *G (6)* represents *Φ (26).* So we can say

$$26 +_{27} k_+ = 6 \Rightarrow k_+ = 6 -_{27} 26 = -20 = 7 \text{ mod } 27$$

	G	W	V	V	Y	G	J	V	K	L	G
Cipher	6	22	21	21	24	6	9	21	10	11	6
$-k_+$	-1	15	14	14	17	-1	2	14	3	4	-20
Mod 27	26	15	14	14	17	26	2	14	3	4	26
Plain	**Φ**	**P**	**O**	**O**	**R**	**Φ**	**C**	**O**	**D**	**E**	**Φ**

(d) Using the affine code with key $(2,11)$ gives

$26 \times 2 + 11 = 63 = 9$ mod 27 and $15 \times 2 + 11 = 41 = 14$ mod 27 so first part would be **JO**

There is a little more security since two different plaintext-ciphertext pairs are required for attack. Given these pairs, two equations may be formed $a_1 k_\times + k_+ =_m b_1$ and $a_2 k_\times + k_+ =_m b_2$. There is a unique solution to these equations if the difference between plaintexts is coprime with the modulus. In part (c) we need to guess another likely pair probably by frequency analysis of more ciphertext.