Written Exam
Information Transmission - EITA30 (EIT100)

Department of Electrical and Information Technology
Lund University

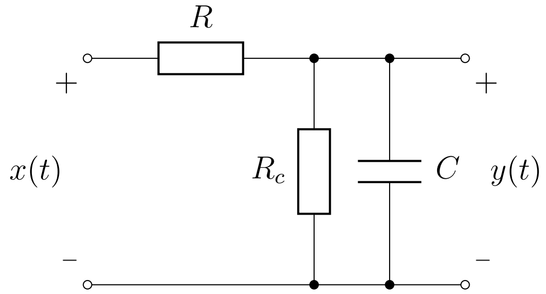
2019-06-03
14.00 – 19.00

*** SOLUTION ***

The exam consists of five problems. 20 of 50 points are required to pass.
Permitted aids: Pocket calculator without any programs, scripts or files stored, formula collection without any notes.

- Write your personal identifier on each page.
- Each solution must be written on separate sheets.
- Your solutions must clearly reveal your method of solution.
- Problems are *not* sorted in order of difficulty.

1. Consider the circuit diagram



where we have a resistor R in series with a realistic model of a capacitor, consisting of an ideal capacitance C in parallel with a resistor R_c. The resistor R_c models leakage of current through the non-ideal capacitor. In an ideal capacitor, $R_c = \infty$. The input and output voltage signals are $x(t)$ and $y(t)$, respectively.

(a) Find the ideal and non-ideal frequency functions, $H_{\text{ideal}}(f)$ and $H_{\text{non-ideal}}(f)$, in terms of R, C and, for the non-ideal case, R_c. (4 p)

Solution: Let's start with the non-ideal case. Voltage division in the $j\omega$ domain gives

$$Y(f) = \frac{Z_1}{Z_1 + Z_2} X(f) = H(f)X(f),$$

where

$$Z_1 = [\text{parallel connection}] = \frac{R_c \frac{1}{j\omega C}}{R_c + \frac{1}{j\omega C}} = \frac{R_c}{j\omega R_c C + 1} \text{ and } Z_2 = R$$

i.e.

$$H_{\text{non-ideal}}(f) = \frac{\frac{R_c}{j\omega R_c C+1}}{R + \frac{R_c}{j\omega R_c C+1}} = \frac{R_c}{R(j\omega R_c C + 1) + R_c} = \boxed{\frac{1}{RC} \frac{1}{j\omega + \frac{1}{R_c C} + \frac{1}{RC}}}$$

For the ideal case, we let $R_c \to \infty$ which makes $\frac{1}{R_c C} + \frac{1}{RC} \to \frac{1}{RC}$ and

$$H_{\text{ideal}}(f) = \boxed{\frac{1}{RC} \frac{1}{j\omega + \frac{1}{RC}}}$$

(b) Find the ideal and non-ideal impulse responses, $h_{\text{ideal}}(t)$ and $h_{\text{non-ideal}}(t)$, of the circuit. (4 p)

Solution: Again, starting with the non-ideal case where

$$H_{\text{non-ideal}}(f) = \frac{1}{RC} \frac{1}{j\omega + \frac{1}{R_c C} + \frac{1}{RC}}$$

we can use Fourier transform property 1 [linearity] and Fourier transform pair (l) [one-sided exponential] to get

$$h_{\text{non-ideal}}(t) = \boxed{\frac{1}{RC} e^{-\left(\frac{1}{R_c C} + \frac{1}{RC}\right)t} u(t)}$$

which with $R_c \to \infty$ gives the ideal impulse response as

$$h_{\text{ideal}}(t) = \boxed{\frac{1}{RC} e^{-\frac{t}{RC}} u(t)}$$

(c) For most practical cases, the leakage resistance R_c in the capacitor is MUCH LARGER than the resistor R we connect in series and it is well motivated to assume the ideal case from above. Further, the product RC is called the *time constant* of the circuit, since it determines how fast the circuit reacts to changes in the input. Assuming that the time constant for our circuit is $RC = 10$ ms, and $R_c \gg R$, find the output $y(t)$ for input $x(t) = 3\cos\omega_0 t$, where $\omega_0 = 100$ rad/s. (2 p)

Solution: At $\omega = \omega_0 = 100$ rad/s and $RC = 10\times 10^{-3}$ s, the ideal frequency function becomes

$$H_{\text{ideal}}(f_0) = \frac{1}{10\times 10^{-3}} \frac{1}{j100 + \frac{1}{10\times 10^{-3}}} = \frac{1}{j+1}$$

which means that the amplitude of our input sinusoid is multiplied by $1/\sqrt{2}$ and its phase is shifted by $-\angle(j+1) = -\frac{\pi}{4}$ rad when going through the filter. The resulting output is

$$y(t) = \boxed{\frac{3}{\sqrt{2}} \cos\left(100t - \frac{\pi}{4}\right).}$$

2. In this problem we consider wireless transmission of a music signal using 16-QAM (Quadrature Amplitude Modulation). The stereo music signal has a bandwidth of 20 kHz and the requirement is that the SNR of the music signal should be better than 60 dB. Assume that a convolutional $R = 2/3$ code is used for the wireless transmission, and that this gives error free transmission over the wireless link (in the sense that it does not influence quality).

   (a) What is the minimum bit rate giving sufficient SNR if standard PCM is used as source coding? (4 p)

   Solution: The total sampling bit rate is given by:

   $$r_{\text{samp}} = 2bf_{\text{samp}} \text{ [bits/sec]}$$

   where 2 is the number of channels (stereo), b the number of bits used per sample (per channel) and f_{samp} is the sampling frequency. We need to find both b and f_{samp}.

   To obtain better than 60 dB SNR, we need b to fulfill $6b - 7.3 \geq 60$. Solving this gives $b \geq (60 + 7.3)/6 \approx 11.22$. Hence, using $b = 12$ bits per sample is sufficient.

   Since the sampled music has a bandwidth of 20 kHz, we need to sample both channels at twice that rate, i.e., we can use $f_{\text{samp}} = 40$ kHz. (In a real system, we would probably select a somewhat larger value to be on the safe side and simplify implementation.)

   Inserting these into the relation above, gives a sampling bit rate of

   $$r_{\text{samp}} = 2 \times 12 \times 40 = \boxed{960 \text{ kbit/sec.}}$$

   (b) What is the symbol time? (3 p)

Solution: First encoding our rate r_{samp} bit/sec sampled signal with a rate R convolutional code and then transmitting it using an M-ary signal constellation, carrying $\log_2 M$ bits per symbol, gives a symbol rate of

$$r_{\text{symb}} = \frac{r_{\text{samp}}}{R \log_2 M}.$$

Combining the result from a) with an $R = 2/3$ convolutional code and an $M = 16$ point signal constellation (16QAM), carrying $\log_2 16 = 4$ bits/symbol, we get

$$r_{\text{symb}} = \frac{960}{2/3 \times 4} = 360 \text{ ksymb/sec.}$$

At this symbol rate, the duration of one symbol is

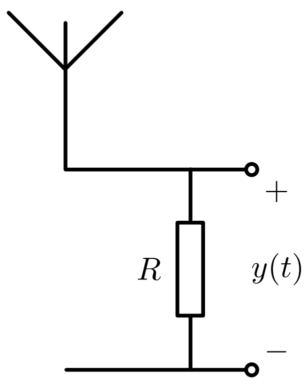
$$T_S = 1/360\,000 \approx \boxed{2.8\ \mu\text{s.}}$$

(c) What is the radio bandwidth if sinc pulses are used for communication? (3 p)

Solution: With sinc-pulses the radio spectrum is rectangular and the bandwidth is equal to the symbol rate, which we already calculated in (b). Hence, the radio bandwidth is

$$BW = \boxed{360 \text{ kHz.}}$$

3. In transmission systems the receiver circuitry can often be modeled as a resistor, a noise source of a certain noise temperature, with $R = 50\ \Omega$ and a certain bandwidth. Assume that the bandwidth is 20 MHz and that the noise temperature is 800 K. The (somewhat oversimplified) model of the receiver antenna is shown in the figure below.



(a) What is the power of the Gaussian noise that is developed across the resistor, expressed in Watt? (4 p)

Solution: The power resulting from a thermal noise source over a certain bandwidth is calculated as $P_n = kBT$, where k is Bolzmann's constant (1.38×10^{-23} J/K), B the bandwidth and T the noise temperature of the source (in K). Combining this with what is given in the problem, we get

$$P_{\text{n}} = 1.38 \times 10^{-23} \times 20 \times 10^6 \times 800 = \boxed{2.2 \times 10^{-13} \text{ W.}}$$

(b) Think of the antenna as a voltage source, it produces a $100\mu V$ radio signal over the resistor. What is the signal power? (3 p)

Solution: Signal power generated by a signal voltage across a resistor is given by

$$P_s = \frac{U^2}{R}$$

which, with our numbers, leads to

$$P_s = \frac{(100 \times 10^{-6})^2}{50} = \boxed{2 \times 10^{-10} \text{ W.}}$$

(c) What is the signal to noise ratio, expressed in dB? (3 p)

Solution: The resulting SNR becomes

$$\text{SNR} = \frac{P_s}{P_n} = \frac{2 \times 10^{-10}}{2.2 \times 10^{-13}} = 909.1 \Longrightarrow \text{SNR}_{\text{dB}} = \boxed{29.6 \text{ dB.}}$$

4. Adrianna wants to send names to Bob using as efficient source coding as possible. After observing Adrianna's behavior over a long time, Bob concluded that the probability of the different names to be sent are the ones shown in the table below.

Name	$P(name)$
Cecilia	0.11
David	0.29
Emmelie	0.20
Frank	0.15
Griselda	0.25

(a) What is the uncertainty of each transmission? (3 p)

Solution: The *uncertainty* of the outcome of a random message U (a name, in this case) is measured by the entropy

$$H(U) = -\sum_i \Pr(U = u_i) \log_2 \Pr(U = u_i) \text{ bit/message.}$$

For this source we have the probabilities

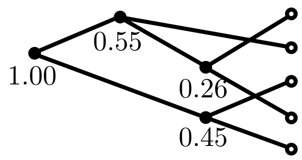
$$\Pr(U = u_i) \in \{0.11, 0.29, 0.20, 0.15, 0.25\}$$

and the corresponding uncertainty/entropy becomes

$$H(U) = -0.11 \log_2 0.11 - 0.29 \log_2 0.29 - 0.20 \log_2 0.20 - 0.15 \log_2 0.15 - 0.25 \log_2 0.25 \approx \boxed{2.24 \text{ bit.}}$$

(b) Derive an efficient bit representation for the case when many names are sent after another using using as few bits as possible on the average for the transmission. Different lengths are allowed if this increases the efficiency. (5 p)

Solution: The "best" way to do this with single messages are to apply the Huffman algorithm, to create a Huffman code. The procedure is illustrated in the figure below.



Prob.	**Message**
0.11	Cecilia
0.29	David
0.20	Emmelie
0.15	Frank
0.25	Griselda

Assigning bits to the paths down from the root of the tree (the one with probability 1.0) gives us a binary variable-length Huffman code. Consequently selecting 0 for the upper branch and 1 for the lower one, we get the code:

Message	Codeword
Cecilia	010
David	00
Emmelie	10
Frank	011
Griselda	11

(c) What is the average word length using your bit representation and how far are you from the optimum representation? (2 p)

Solution: The average code-word length can be calculated as the sum of probabilities for all internal nodes in the Huffman tree (including the root node). This gives an average code-word length $\bar{W} = 1.00 + 0.55 + 0.45 + 0.26 = 2.26$ bit/message. This is very close to the entropy 2.24 bit/message, within 1%, which is the ultimate limit.

The representation can be made even more efficient by grouping messages into blocks and applying Huffman coding on the blocks, but when we are within 1% of the optimum, this is hardly worth the extra effort.

5. A two-key RSA crypto system is set up with the public parameters $n = 7849$ and $e = 25$.

(a) Find the cipher text C corresponding to plain text $P = 1111$. (4 p)

Solution: Encryption is performed as $C \equiv P^e \mod n$, which in our case results in

$$C \equiv 1111^{25} = 1111^{16+8+1} \mod 7849$$

where

$$\begin{aligned}
1111^1 &\equiv 1111 \mod 7849 \\
1111^2 &\equiv 2028 \mod 7849 \\
1111^4 &\equiv 2028^2 \equiv 7757 \mod 7849 \\
1111^8 &\equiv 7757^2 \equiv 615 \mod 7849 \\
1111^{16} &\equiv 615^2 \equiv 1473 \mod 7849
\end{aligned}$$

which gives

$$C \equiv 1111^{25} = 1473 \times 615 \times 1111 \equiv \boxed{3471 \mod 7849}$$

(b) Unfortunately, you have forgotten the decryption exponent d. However, since you selected the key from the beginning, you know that 47 is a factor of 7849. Use this knowledge to calculate the decryption exponent d again. (6 p)

Solution: Using that 47 is one of the prime factors of $n = 7849$, we easily find the other prime factor as 167. With these we can calculate Euler's totient function

$$\Phi(7849) = (47 - 1)(167 - 1) = 7636$$

which we use to calculate our decryption exponent d as the multiplicative inverse of the encryption exponent e, modulo $\Phi(n)$, through solving $de + t\Phi(n) = 1$. We start with Euclide's algorithm for calculating the gcd:

$$\begin{aligned} 7636 &= 305 \cdot 25 + 11 \\ 25 &= 2 \cdot 11 + 3 \\ 11 &= 3 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 (\text{finished}) \end{aligned}$$

and then in the reverse direction:

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 \\ 1 &= 3 - 1 \cdot (11 - 3 \cdot 3) = 4 \cdot 3 - 1 \cdot 11 \\ 1 &= 4 \cdot (25 - 2 \cdot 11) - 1 \cdot 11 = 4 \cdot 25 - 9 \cdot 11 \\ 1 &= 4 \cdot 25 - 9 \cdot (7636 - 305 \cdot 25) = \underbrace{2749}_{d} \cdot \underbrace{25}_{e} - \underbrace{9}_{t} \cdot \underbrace{7636}_{\Phi(n)} \end{aligned}$$

where we identify $d = 2749$.