Written Exam
Information Transmission - EITA30/EIT100

Department of Electrical and Information Technology
Lund University

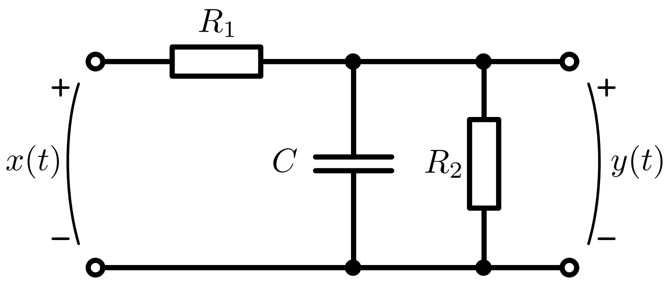
2020-06-01
14.00 – 19.00

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.

1. Consider this circuit, built up by two resistors, R_1 [Ω] and R_2 [Ω], and a capacitor, C [F]. The input signal is $x(t)$ [V] and the output signal $y(t)$ [V].



Answer the following questions:

(a) What is the frequency function $H(f)$ of the circuit, expressed in capacitance C and resistances R_1 and R_2? (3 p)

(b) Assume that the input is a sinus-signal with angular frequency ω and amplitude A, i.e., $x(t) = A\sin(\omega t)$. How large is the amplitude of the output $y(t)$ when the frequency is

i. low, i.e., when $\omega \to 0$, and (1 p)

ii. high, i.e., when $\omega \to \infty$? (1 p)

(c) For some reason, a critical requirement is that no frequency component of the input signal $x(t)$ is delayed more than 10 ms by the circuit. Let's approach this in two steps.

Hint: *With input* $x(t) = \sin(\omega t)$ *the output will be on the form* $y(t) = |H(f)|\sin(\omega t + \phi(\omega))$, *which can be re-written as* $y(t) = |H(f)|\sin(\omega(t + \phi(\omega)/\omega))$.

i. Determine the frequency-dependent time delay $\Delta(\omega)$ (in seconds) imposed by the circuit at angular frequency ω, in terms of R_1, R_2 and C. (2 p)

ii. Use $\Delta(\omega)$ to find an expression (that includes R_1, R_2, and C), that ensures a maximum delay of 10 ms (at any frequency). (1 p)

(d) This filter was designed by someone who wanted to remove some high-frequency disturbances from $x(t)$, making $y(t)$ a "cleaned" version of $x(t)$. The wanted part of $x(t)$ has lower frequencies than the unwanted disturbance. To get "as much as possible" of the wanted (low-frequency) signal to go through to $y(t)$, the designer decided to set $R_1 = 0$. Is this a good move? Motivate your answer clearly. (2 p)

2. Rectangular basis-pulses are used to transmit a binary sequence, where amplitude $-A$ represents "0" and amplitude $+A$ represents "1". This constitutes 2-ASK transmission and the transmission rate is set to 384 kbit/s. Transmission takes place in the base-band, i.e., *without* up-conversion to (modulation on) a carrier.

(a) Sketch, as accurately as possible, the transmitted signal produced by the binary sequence $\mathbf{b} = (1\ 1\ 0\ 1)$. The sketch should include accurate amplitude and time scales. (For control purposes, enter the max/min values of the resulting signal and the symbol time in the corresponding text boxes below.) (3 p)

(b) Sketch the spectrum of the transmitted signal, as accurately as you can, assuming that random independent symbols are transmitted. The frequency scale and general shape of the spectrum are important to get right, not absolute amplitude levels. (For control purposes, enter the one-sided bandwidth, in terms of the frequency of the first spectrum zero, in the text box below.) (4 p)

(c) Now, let's assume that 8-ASK (eight different amplitude levels, e.g. $\pm A$, $\pm 3A$, $\pm 5A$ and $\pm 7A$) is used, instead of 2-ASK, also with rectangular pulses. What is the new symbol time, given that the bit rate remains unchanged? How is the spectrum bandwidth affected by this choice of modulation, compared to the 2-ASK case? Motivate clearly. (3 p)

3. Variable-length prefix-free source codes can often be made more efficient (perform closer to what is optimal in terms of average number of bits/symbol for a given source) by encoding several source symbols together, rather than encoding them one-by-one. This, however, brings about additional "complexity" when creating the codewords (there are more of them). Let's investigate this in some detail, under the assumption that our source (stochastic variable) U has M different outcomes/symbols $\{U = u_i\}$, with respective probabilities $P_U(u_i)$, for $i = 1, 2, \ldots, M$. The sequences generated by the source, $\mathbf{U} = U_1 U_2 U_3 \ldots$, are composed of independently drawn outcomes from U.

For this problem we use only $M = 4$ different symbols, but have two different probability distributions, $P_U^{(A)}(u_i)$ and $P_U^{(B)}(u_i)$, indicated by superscripts (A) and (B), respectively:

U	$P_U^{(A)}(u_i)$	$P_U^{(B)}(u_i)$
u_1	0.500	0.500
u_2	0.239	0.250
u_3	0.161	0.125
u_4	0.100	0.125

(a) What is the uncertainty of the source, for each of the two probability distributions, (A) and (B)? (3 p)

(b) Derive optimal variable-length prefix-free binary code words, for each of the two probability distributions, (A) and (B), when encoding symbol-by-symbol. Calculate the corresponding average code-word lengths, $\overline{W}^{(A)}$ and $\overline{W}^{(B)}$, and comment on how close they are to what is ultimately possible and if grouping more and more symbols together potentially can improve the efficiency? (4 p)

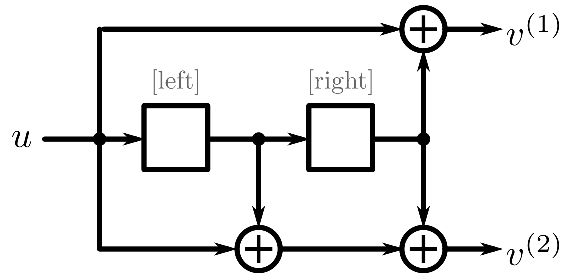
(c) Compare the expression for uncertainty/entropy, $H(U)$, with this expression,

$$\overline{W}^{(*)} = \sum_{i=1}^{M} P_U^{(*)}(u_i) w_i^{(*)},$$

for calculating average code-word length. Here (*) indicates either (A) or (B), and $w_i^{(*)}$ is the length of the code word for symbol u_i. What conclusion do you draw about which type of probability distributions lead to symbol-by-symbol Huffman codes that cannot be improved by grouping more symbols together? (3 p)

Hint: *Studying the two probability distributions, (A) and (B), and the outcome of (b) may help you to draw the right conclusion.*

4. Consider the rate $R = 1/2$ convolutional encoder shown below.



(a) Draw one complete trellis stage for the above encoder, with states [left][right] in the order 00, 01, 10, 11, from top to bottom. Include all state transitions, as well as the encoder output $v^{(1)}v^{(2)}$ at each transition. (For control purposes, enter the two encoder outputs when exiting state 11 in the text boxes below.) (3 p)

(b) Given the input sequence $\boldsymbol{u} = (u_1\ u_2\ \ldots\ u_6) = (1\ 0\ 1\ 1\ 0\ 0)$, what is the corresponding code word $\boldsymbol{v} = (v_1^{(1)}v_1^{(2)}\ v_2^{(1)}v_2^{(2)}\ \ldots)$? (The encoder starts in the all-zero state and the last two zeros in the sequence are termination bits, used to force the encoder back to the all-zero state.) (2 p)

(c) Show clearly how you execute the Viterbi algorithm to decode the received sequence $\boldsymbol{r} = (01\ 01\ 00\ 10\ 00\ 10)$. What is the resulting decoded code-sequence $\hat{\boldsymbol{v}} = (\hat{v}_1^{(1)}\hat{v}_1^{(2)}\ \hat{v}_2^{(1)}\hat{v}_2^{(2)}\ \ldots)$? (5 p)

5. Consider an RSA public key crypto system with the public encryption key $(n, e) = (697, 21)$. Find the plaintext P corresponding to the ciphertext $C = 421$. Motivate your answer carefully, by showing all calculation steps in detail. (10 p)

Hint: *One of the factors of* n *is* $p = 41$.