Exam Solution
Total score: 49/49

+1/1/60+

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Midterm Exam

Advanced Information, Computation, Communication II

April 9, 2019

15h20 – 17h00

Important Notes

- Due to another exam, this midterm will end at 17h00 sharp.
- No document or electronic device is allowed.
- For each question, there is exactly one correct answer. We assign negative points to the wrong answers, in such a way that a person that chooses at random according to a uniform distribution over the possible choices gains 0 points in average. (Same as not answering.)
- Mark your answer with a thick 'X' in the corresponding box. If you want to change your answer, color the box completely and mark the new answer with an 'X'.
- Each page has a code on top of it (see the top of this page). Do not write on it.
- For technical reasons, pencils are not allowed.
- All entropies are in bits.

Room:
Seat:

Student Name / Sciper no.:
Exam Solution

Problem 1 [2 points]

A 4-ary source S produces iid symbols following the distribution $p_S(0) = 1/2$, $p_S(1) = 1/4$, $p_S(2) = 1/8$, and $p_S(3) = 1/8$. For any integer $n > 0$, let S^n be a sequence of n symbols produced by the source S. What is the probability of the most probable sequence S^n? Check one:

- ☐ $(\frac{1}{32})^n$
- ☒ $(\frac{1}{2})^n$
- ☐ $(\frac{1}{4})^n$
- ☐ $(\frac{1}{16})^n$
- ☐ $(\frac{1}{8})^n$

2/2

Problem 2 [2 points]

Consider the binary source code $\mathcal{C} = \{0, 01, 10\}$ for a ternary random variable. Answer the following True/False questions [1 point each]:

1/1 ☐ True ☒ False The code is uniquely decodable

1/1 ☐ True ☒ False The code is instantaneous

Problem 3 [4 points]

A given binary prefix-free code consists of codewords of lengths 2, 2, 2, 3, 4. Is it possible to add one codeword to this code and guarantee that the new code is prefix-free?

- ☐ Yes, its maximum length is 4
- ☐ Yes, the length has to be exactly 4

4/4

- ☐ It depends on the given code
- ☒ Yes, its minimum length is 4
- ☐ No

Problem 4 [4 points]

Consider a random variable X which takes on four possible values with probabilities 1/3, 1/3, 1/4 and 1/12. Assuming that we encode one symbol at a time, what is the smallest average codeword length which a binary uniquely decodable code can achieve for the random variable X? Check one:

- ☐ 2.2
- ☐ 2.18

4/4

- ☐ 1.6
- ☐ 1.8
- ☒ 2

Problem 5 [2.5 points]
Consider a code $\mathcal{C}$ used for source coding. Answer the following True/False questions [0.5 point each]:

0.5/0.5	☒ True	☐ False	$\mathcal{C}$ does not satisfy Kraft's inequality $\Rightarrow$ $\mathcal{C}$ is with prefix
0.5/0.5	☐ True	☒ False	$\mathcal{C}$ satisfies Kraft's inequality $\Rightarrow$ $\mathcal{C}$ is uniquely decodable
0.5/0.5	☐ True	☒ False	$\mathcal{C}$ is with prefix $\Rightarrow$ $\mathcal{C}$ is not uniquely decodable
0.5/0.5	☐ True	☒ False	$\mathcal{C}$ is with prefix $\Rightarrow$ $\mathcal{C}$ does not satisfy Kraft's inequality
0.5/0.5	☒ True	☐ False	The codeword lengths do not satisfy Kraft's inequality $\Rightarrow$ $\mathcal{C}$ is not uniquely decodable

Problem 6 [3 points]
Consider two random variables X and Y. Which of the following statements is always true? Check one:

- ☐ If $H(X) + H(Y) > H(X,Y)$, then X and Y are independent.
- ☒ If $H(X) - H(X|Y) = 0$, then X and Y are independent. 3/3
- ☐ If $H(X|Y) = 0$, then X and Y are independent.
- ☐ If $H(X,Y) = 0$, then X and Y are independent.

Problem 7 [4 points]
Consider two random variables X and Y over the alphabet $\{0,1,2,3\}$ with the joint probability distribution $p_{X,Y}(x,y)$ given in the table below:

$p_{X,Y}(x,y)$	0	1	2	3
0	1/8	1/16	1/16	1/4
1	1/16	1/8	1/16	0
2	1/32	1/32	1/16	0
3	1/32	1/32	1/16	0

The entropy $H(X,Y)$ is (check one):

- ☐ $\frac{31}{8}$ bits
- ☐ 2 bits
- ☒ $\frac{27}{8}$ bits 4/4
- ☐ $\frac{7}{4}$ bits
- ☐ $\frac{13}{4}$ bits

Problem 8 [5 points]
Let X and Y be independent and uniformly distributed random variables taking values in $\{0,1\}$ and let $Z = (X+Y) \mod 2$. Answer the following True/False questions [1 point each]:

1/1	☐ True	☒ False	$H(X,Y,Z) = H(X)$
1/1	☒ True	☐ False	$H(X,Y,Z) = H(X) + H(Y)$
1/1	☐ True	☒ False	$H(X,Z) < H(X) + H(Z)$
1/1	☐ True	☒ False	$H(X,Y,Z) = H(X) + H(Y) + H(Z)$
1/1	☐ True	☒ False	$H(Z\|X,Y) = H(Z)$

Problem 9 [5 points]

Let $S_1, S_2, \ldots$ be a sequence of independent (but not identically distributed) random variables taking values in $\{0, 1\}$, where $p_{S_n}(1) = \frac{1}{n}$. We denote by $H^*(\mathcal{S})$ and $H(\mathcal{S})$ the entropy rate and the entropy of a symbol of this source, respectively. Answer the following True/False questions [1 point each]:

1/1	☐ True	☒ False	$H^*(\mathcal{S})$ and $H(\mathcal{S})$ are not defined since the source is not stationary
1/1	☐ True	☒ False	$H(\mathcal{S})$ is defined, but not $H^*(\mathcal{S})$
1/1	☐ True	☒ False	$H^*(\mathcal{S}) < H(\mathcal{S}) \leq 1$
1/1	☐ True	☒ False	$H^*(\mathcal{S})$ is defined, but not $H(\mathcal{S})$
1/1	☒ True	☐ False	$H^*(\mathcal{S}) = H(\mathcal{S}) = 0$

Problem 10 [4 points]

What is the plaintext corresponding to the ciphertext SRAYVPOGR if the Vigenère cipher is used and the key is KEY? (Consider only the 26 characters of the English alphabet and the mapping is A $\rightarrow$ 0, B $\rightarrow$ 1, ..., Z $\rightarrow$ 25.) Check one:

- ☐ INCERTAIN
- ☐ GOODYEARS
- 4/4 ☒ INCORRECT
- ☐ INCREASE
- ☐ INCAPABLE

Problem 11 [3 points]

The plaintext t of a symmetric-key cryptosystem is a length 1000 binary string. To generate the key, you choose at random (uniform distribution) a number $y \in \mathcal{Y} = \{1, 2, \ldots, 2^{1000}\}$ and then compute the key $k = f(y)$, where $f : \mathcal{Y} \rightarrow \mathcal{Y}$ is a one-way function (one-to-one onto). Does the system achieve perfect secrecy? Check one:

- ☐ No, because with a one-way function you have only computational security
- ☐ Yes
- 3/3 ☐ Yes, because the entropy of the key exceeds that of the plaintext
- ☒ It can, but it depends on missing details.

Problem 12 [2 points]

Which of the following statements is always true for the one-time pad with key $K \in \{0, 1\}^n$ and plaintext $T \in \{0, 1\}^n$? Check one:

- ☐ $H(K) = n$ and $H(T) = n$
- 2/2 ☐ $H(K) = 2^n$ and $H(T) \leq 2^n$
- ☒ $H(K) = n$ and $H(T) \leq n$

Problem 13 [4 points]

Which, if **any**, one of the following is a MOD97-10 number?

- $98^3 \times 99 \times 104^2$
- $98^3 \times 99 \times 104^2 + 13$
- $98^3 \times 99 \times 104^2 + 2$

- [ ] The third
- [x] The first
- [ ] None
- [ ] The second
- [ ] All three

4/4

Problem 14 [4.5 points]

Consider the following two independent equations:

$$x[162]_{437} - [383]_{437} = [0]_{437},$$
$$x[152]_{437} + [413]_{437} = [0]_{437}.$$

Which of the following statements is true? Check one:

- [ ] Both have a unique solution
- [x] The first has a unique solution but not the second
- [ ] The second has a unique solution but not the first
- [ ] Neither one has a unique solution

4.5/4.5