Student
Total score: 87/87

+1/1/60+

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Final Exam

Advanced Information, Computation, Communication II

August 10, 2020

16h15 – 19h15

Important Notes

- 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, use white correction tape/pen 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: **Campus-I**
Seat: **1**

Student Name / Sciper no.:
Student

Problem 1 [4 points]
Consider a random variable S described by the following probability distribution:

Alphabet Symbol	a	b	c	d	e	f
Probability	0.04	0.06	0.1	0.2	0.2	0.4

Let $H(S)$ be the entropy of S. We consider only uniquely-decodable codes and a code is considered to be optimal if no code can achieve a smaller average codeword-length.
Answer the following True/False questions [1 point each]:

1 [ ] True [x] False The average codeword-length of an optimal binary code for S is $H(S)$
1 [x] True [ ] False The set of codeword lengths of a binary Huffman code for S is not unique
1 [ ] True [x] False The average codeword-length of an optimal binary code for S is 1.3 bits
1 [x] True [ ] False There exists a binary uniquely-decodable code for S with codeword lengths $\{1,2,3,4,5,5\}$

Problem 2 [6.25 points]
Consider two dice: a fair one and a rigged one which rolls only 1. We roll the two dice and let X be the sum of the outcomes. Let $Y = (X \mod 6)$ and $Z = (Y \mod 4)$.
Answer the following True/False questions [1.25 points each]:

1.25 [x] True [ ] False $H(X,Y) > H(Z)$
1.25 [ ] True [x] False $H(Y) < H(Z)$
1.25 [ ] True [x] False $H(X,Y) = H(X|Y)$
1.25 [ ] True [x] False $H(Y,Z) = H(Y) + H(Z)$
1.25 [ ] True [x] False $H(X,Z) < H(X,Y)$

Problem 3 [7 points]
Consider two dice: a fair one and a special one which rolls only 0. We pick one of the dice at random and roll it indefinitely. The sequence of rolls can be modelled as the output of the source $\mathcal{S} = S_1, S_2, \ldots$
Let $H(S)$ be the entropy of a symbol and $H^*(\mathcal{S})$ be the entropy rate.
Answer the following True/False questions [1 point each, unless otherwise specified]:

1 [x] True [ ] False $\lim_{n\to\infty} \frac{H(S_1,S_2,\ldots,S_n)}{n} < 3$
2 [x] True [ ] False $H(S) > 2$ [2 points]
1 [ ] True [x] False S_1 and S_2 are independent
1 [x] True [ ] False $H(S_1) = H(S_2)$
2 [x] True [ ] False $H^*(\mathcal{S}) = \frac{1}{2}\log_2 6$ [2 points]

Problem 4 [3 points]
Let $\mathcal{S}$ be a regular binary source which produces independent and identically distributed symbols. Assume you compress $\mathcal{S}$ using a binary Huffman code which operates on blocks of n symbols, for some fixed positive integer n. Answer the following True/False questions [1.5 points each]:

1.5 ☐ True ☒ False — If the average codeword-length per symbol of the Huffman code is 1, then $\mathcal{S}$ produces symbols with uniform distribution

1.5 ☒ True ☐ False — If $\mathcal{S}$ produces symbols with uniform distribution, then the average codeword-length per symbol of the Huffman code is 1

Problem 5 [4 points]
Given a source code $\mathcal{C}$ that does *not* satisfy Kraft's inequality, we want to modify it in such a way that the new code $\mathcal{C}'$ satisfies Kraft's inequality. Answer the following True/False questions [1 point each]:

1 ☐ True ☒ False — We can always obtain $\mathcal{C}'$ by shortening one or more codewords of $\mathcal{C}$. The result is guaranteed to be prefix-free.

1 ☐ True ☒ False — We can always obtain $\mathcal{C}'$ by adding a few codewords to $\mathcal{C}$

1 ☒ True ☐ False — We can always obtain $\mathcal{C}'$ by appending a suffix to one or more codewords of $\mathcal{C}$

1 ☐ True ☒ False — We can always obtain $\mathcal{C}'$ by shortening one or more codewords of $\mathcal{C}$. The result may or may not be prefix-free.

Problem 6 [2.25 points]
Let X be uniformly distributed over $\{0, 1, 2, ..., 7\}$. Define random variables $Y = (X \mod 2)$ and $Z = (X \mod 6)$. Find $H(Y) + H(Z)$. Check one:

☐ 4.5
☐ 2
☐ 4
☒ 3.5

2.25

Problem 7 [4 points]
Let $\mathcal{S} = S_0, S_1, S_2, \ldots$ be an infinite source where $S_i \in \{H, T\}$ are coin flips defined as follows:

$$S_0 \in \{H, T\} \text{ is a fair coin flip;}$$

$$S_i = \begin{cases} H & \text{if } S_{i-1} = T, \\ T & \text{if } S_{i-1} = H \end{cases} \quad \text{for all } i \geq 1.$$

Answer the following True/False questions [1 point each]:

1 ☒ True ☐ False — $H(S_i) = 1$ for all $i \geq 0$

1 ☒ True ☐ False — $\mathcal{S}$ is regular

1 ☒ True ☐ False — $H(\mathcal{S}) = 1$

1 ☐ True ☒ False — $H^*(\mathcal{S}) = 1$

Problem 8 [4 points]
We are looking for an integer k such that $(\mathbb{Z}/k\mathbb{Z}, +)$ is isomorphic to $(\mathbb{Z}/12\mathbb{Z}^*, \cdot)$. Check one:

- [x] Such k does not exist
- [ ] $k = 4$
- 4 [ ] $k = 11$
- [ ] There is more than one valid value for k
- [ ] $k = 12$

Problem 9 [6 points]
Alice and Bob would like to communicate using a symmetric-key cryptosystem. To exchange the key over the public channel, they use Diffie and Hellman public key-distribution scheme seen in class. Assume that we work within the group $(\mathbb{Z}/7\mathbb{Z}^*, \cdot)$ with the generator $g = 3$. The secret number picked by Alice is $a = 4$ and the one picked by Bob is $b = 5$.
Answer the following True/False questions [2 points each]:

2 [ ] True [x] False There is no need to specify the generator since $(\mathbb{Z}/7\mathbb{Z}^*, \cdot)$ has only one generator

2 [x] True [ ] False Alice's public key (i.e. her entry in the publicly available directory) is 4

2 [ ] True [x] False The shared key is 3

Problem 10 [4 points]
Let (m, e) be an RSA public encoding key and let c_1 and c_2 be the encryptions of the messages t_1 and t_2 respectively. All operations are in $\mathbb{Z}/m\mathbb{Z}$ and the multiplicative inverse of t_2, denoted t_2^{-1} is assumed to exist. Answer the following True/False questions [1 point each]:

1 [ ] True [x] False Encryption of $t_1 + t_2$ is $c_1 + c_2$

1 [x] True [ ] False Encryption of $t_1 t_2$ is $c_1 c_2$

1 [x] True [ ] False Encryption of $t_1 t_2^{-1}$ is $c_1 c_2^{-1}$

1 [ ] True [x] False Encryption of $t_1 - t_2$ is $c_1 - c_2$

Problem 11 [4 points]
Let $(m, e) = (221, 77)$ be an RSA public encoding key and let $c = 15$ be the encryption of a message $t \in \mathbb{Z}/m\mathbb{Z}$. Find t (check one):

- [x] $t = 19$
- [ ] $t = 60$
- [ ] $t = 13$ 4
- [ ] $t = 27$
- [ ] $t = 58$

Problem 12 [3 points]
Answer the following True/False questions [1 point each]:

1	☐ True	☒ False	$16^{123} \mod 17 = 1$
1	☐ True	☒ False	$73561 \mod 9 = 7$
1	☒ True	☐ False	$6487248918923131514 \mod 16 = 10$

Problem 13 [6 points]
Let T, K, C be elements of a finite commutative group $(G, \star)$ and let $C = T \star K$, where T represents the plaintext, K the key, and C the cryptogram. The plaintext and the key are selected independently. Answer the following True/False questions [1.5 points each]:

1.5	☐ True	☒ False	If T is uniformly distributed, then the system achieves perfect secrecy
1.5	☐ True	☒ False	It is not possible to achieve perfect secrecy with any finite commutative group $(G, \star)$
1.5	☒ True	☐ False	If K is uniformly distributed, then the system achieves perfect secrecy
1.5	☐ True	☒ False	The system achieves perfect secrecy only if both T and K are uniformly distributed

Problem 14 [5 points]
Consider an (n, k) linear code $\mathcal{C}$, with a parity-check matrix H. Answer the following True/False questions [1.25 points each]:

1.25 ☐ True ☒ False — If there exists a collection of $n-k+1$ columns of H which are linearly dependent, then the code is MDS

1.25 ☒ True ☐ False — If there exists a collection of $n-k$ columns of H which are linearly dependent, then the code is not MDS

1.25 ☒ True ☐ False — There exists a collection of $n-k+1$ columns of H which are linearly dependent

1.25 ☐ True ☒ False — All collections of $n-k$ columns of H are linearly dependent

Problem 15 [3 points]
Let

$$G_{\text{sys}} = \begin{pmatrix} 1 & 0 & 0 & 1 & 3 \\ 0 & 1 & 0 & 2 & 2 \\ 0 & 0 & 1 & 3 & 1 \end{pmatrix}$$

be the generator matrix in systematic form for a Reed-Solomon code over $\mathbb{F}_5 = (\mathbb{Z}/5\mathbb{Z}, +, \cdot)$. If a codeword is sent over an erasure channel and we received $(?, 3, 2, 4, ?)$, what is the transmitted codeword? Check one:

- ☒ $(2, 3, 2, 4, 4)$
- ☐ $(2, 3, 2, 4, 2)$

3

- ☐ $(4, 3, 2, 4, 0)$
- ☐ $(4, 3, 2, 4, 1)$

Problem 16 [4 points]
A malevolent organization wants to hand-deliver some message $(u_1, \ldots, u_8) \in \mathbb{F}_{16}^8$ to a specific address. Sending a single messenger with the entire message is too risky, as there is some chance that the police will recognize and intercept the messenger. So, they transform the original $(u_1, \ldots, u_8)$ into some derived message $(v_1, \ldots, v_n) \in \mathbb{F}_{16}^n$ and use n messengers, each carrying one component of $(v_1, \ldots, v_n)$. (So messenger i carries v_i, $i = 1, \ldots, n$). What is the smallest n if we want to be sure that the original message arrives to destination and we are confident that at most half the messengers can be intercepted? (The sender and the recipient have agreed on the transformation to be used.) Check one:

- ☐ $n = 12$
- ☐ $n = 4$
- 4 ☒ $n = 16$
- ☐ $n = 8$
- ☐ $n = 10$

Problem 17 [7.5 points]
Let the generator matrix of a Reed-Solomon code over some finite field $\mathbb{F}$ be

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ a_1 & a_2 & a_3 & \cdots & a_n \\ (a_1)^2 & (a_2)^2 & (a_3)^2 & \cdots & (a_n)^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (a_1)^{k-1} & (a_2)^{k-1} & (a_3)^{k-1} & \cdots & (a_n)^{k-1} \end{pmatrix},$$

where $a_1, a_2, \ldots, a_n$ are distinct field elements and $n > k$. Answer the following True/False questions [1.5 points each].

Which of the following transformations always lead to a generator matrix for a Reed-Solomon code, possibly with different parameters?

1.5 [X] True [ ] False permute two columns of G
1.5 [X] True [ ] False add a row of G to a different row
1.5 [ ] True [X] False remove the top row of G
1.5 [X] True [ ] False permute two rows of G
1.5 [X] True [ ] False remove the bottom row of G

Problem 18 [5 points]
Consider the block code $C = \{(0,0,0,0,0), (1,1,2,2,2), (2,2,1,1,1), (2,2,2,2,0)\}$ defined over $\mathbb{F}_3 = (\mathbb{Z}/3\mathbb{Z}, +, \cdot)$. Assume that we use a minimum-distance decoder.
Answer the following True/False questions [1.25 points each]:

1.25 [ ] True [X] False C is linear
1.25 [ ] True [X] False C can correct all the errors of weight 2
1.25 [X] True [ ] False There exists a codeword with 4 erasures that a decoder would reconstruct correctly
1.25 [ ] True [X] False C can correct all erasures of weight 3

Problem 19 [5 points]
Consider a finite field $\mathbb{F}$ and k pairs $(a_i, y_i) \in \mathbb{F}^2$. We are looking for a polynomial $P(x)$ over $\mathbb{F}$ of degree at most $k-1$ such that $P(a_i) = y_i$, $i = 1, \ldots, k$.
Answer the following True/False questions [1.25 points each]:

1.25 [X] True [ ] False If a_i are all distinct, such a polynomial exists and it is unique
1.25 [ ] True [X] False If a_i are all distinct, but y_i are not, such a polynomial does not exist
1.25 [X] True [ ] False If y_i are all distinct, but a_i are not, such a polynomial does not exist
1.25 [ ] True [X] False If a_i are not all distinct, depending on the values of y_i, such a polynomial might or might not exist. If it exists, it is unique.

End of the exam. This page is empty.